

# ZTE Cybersecurity White Paper

Provide customers with end-to-end security assurance for products and services

Security in DNA, Trust through Transparency

Chief Security: Officer of ZTE Corporation: Zhong Hong

ZTE Corporation

March, 2019



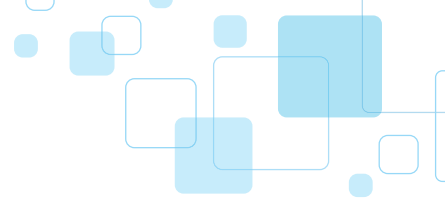
## Written by the author:

This white paper describes ZTE's opinion, principles, strategies, and practices in terms of cybersecurity. This paper was jointly developed by many colleagues.

I'd like to extend my appreciation to those who have made important contributions to the drafting of this document: Cao Kunpeng, Cheng Junhua, Chi Yifei, Gao Ruixin, He Ying, Hua Guohong, Li Rongkun, Liu Risheng, Liu Yan, Liu Yan, Long Hao, Xu Guorong, Meng Zhuli, Nie Yongli, Ping Li, Song Weiqiang, Ma Zhiyuan, Wang Huagang, Wang Lin, Wang Yuzhong, Wei Yinxing, Yang Tiejian, Zhang Can, Zhang Jie, Zhang Rui, Zhao Shanhong, Zheng Jun, Zhou Jihua, and others who made direct or indirect contributions to this white paper.

**Zhong Hong**

Chief Security Officer of ZTE Corporation



# Contents

<b>Preface</b>	<b>04</b>
<b>Executive Summary</b>	<b>05</b>
<b>ZTE's Cybersecurity Strategy</b>	<b>10</b>
<b>End-to-End Cybersecurity Practices</b>	<b>14</b>
<b>Cybersecurity Governance Architecture Based on Three Lines of Defense</b>	<b>15</b>
<b>Cybersecurity Specification System</b>	<b>17</b>
<b>R&amp;D Security</b>	<b>18</b>
R&D Security Procedures and Organizations	18
Concept Phase	20
Plan Phase	20
Development Phase	21
Testing Phase	21
Release Phase	21
Third-Party Component Security Governance	22
Continuous Security Delivery	22
<b>Supply Chain Security</b>	<b>23</b>
Supplier and Material Management	24
Production Security and Return-for-repair Security	26
Warehousing and Logistics Security	27
<b>Delivery Security</b>	<b>28</b>
Three Phases of Delivery Security	29
Subcontractor Management	30



<b>Information Security</b>	<b>31</b>
Information Classification	32
Personnel Security	32
Physical Security	32
IT Security	33
<b>Personal Data Protection</b>	<b>35</b>
Data Protection Compliance System	36
Data Breach Protection Response Mechanism	37
Data Protection Solution Practice	38
<b>Security Incident Management</b>	<b>39</b>
Responses to Cybersecurity Incidents	39
Handling Process for Cybersecurity Vulnerabilities	40
<b>Business Continuity Management</b>	<b>42</b>
BCM in R&D	42
BCM in Supply Chain	43
BCM in Engineering Services	43
BCM in IT Systems	43
<b>Independent Security Assessment</b>	<b>44</b>
Control Mechanism for Independent Security Assessment	44
Process of Independent Security Assessment	45
Methods Applied in Independent Security Assessment	45
<b>Security Audit</b>	<b>46</b>
<b>Cybersecurity Labs and External Cooperation</b>	<b>47</b>
<b>Look Forward and Advance Together</b>	<b>48</b>
<b>Appendix: Major Cybersecurity Events of ZTE</b>	<b>50</b>



# Preface



*Cyberspace has become an integral part of modern society, impacting all aspects of people's daily life. Due to the open and wide spread nature of technology, cyberspace is an easy target, easily attacked or damaged due to the asymmetrical nature of cyber threats and defenses and the inherent cyberspace vulnerabilities. Closely related to every system and individual that rely on networks, cybersecurity has already become a concern for governments, operators, and users around the world.*

*Telecommunications equipment and IT systems are the two main supporting infrastructures platforms of cyberspace. As an integrated telecommunications solution provider for the international markets, ZTE has been insisting on the following principles in terms of cybersecurity:*

*Cybersecurity is one of the highest priorities of ZTE's product development and delivery business units and as a result ZTE has established a holistic cybersecurity governance structure underpinning the company's development strategy. The plan, is supported by relevant laws, regulations, and standards, while fostering good security awareness for all employees and emphasizing the importance of security across the entire end-to-end process. The company attaches great importance to customers' security values, abides by the relevant laws and regulations within the realm of cybersecurity, and ensures end-to-end delivery of secure and reliable products and services.*

*ZTE continues to communicate and cooperate with operators, regulatory agencies, partners, and other stakeholders in an open and transparent manner with respect to continuous improvement in our cybersecurity practices. In accordance with laws and regulations, ZTE respects legitimate rights and interests of users and end users, and keeps innovating and improving our management and technical practices. Ultimately, ZTE is committed to providing customers with secure and trustworthy products and services, while creating a secure cyber environment together with all stakeholders and maintaining a sound security order for cyberspace.*







*The 5G era has been started. Technologies like cloud computing, the Internet of Things (IoT), big data, and AI are gradually booming in the market. These new technologies bring about a new industry revolution together with significant cybersecurity concerns*

*Insisting on openness, transparency, and trust, ZTE implements its cybersecurity governance via a top-down approach.*



The 5G era has been started. Technologies like cloud computing, the Internet of Things (IoT), big data, and AI are gradually booming in the market. These new technologies bring about a new industry revolution together with significant cybersecurity concerns, with growing cybersecurity threats and cybercrimes becoming rampant around the world. The 2018 Verizon Data Breach Investigations Report<sup>1</sup> elaborated on cybersecurity situations in many industries worldwide. The report claims more than 53,000 cybersecurity incidents, and 2216 confirmed data breach incidents in 2018 being reported during the investigation. Information systems may have a number of security vulnerabilities, as of February 2019, exposed CVE vulnerabilities<sup>2</sup> reached 112364, of which 13.5% were critical vulnerabilities and 23.0% were high ones.

Telecommunications equipment and systems composed of information communications equipment are crucial for the growth of cyberspace. Due to the asymmetrical nature of security threats and defenses and the inherent vulnerabilities existing in the system, these communication infrastructures are easily attacked and damaged, putting the entire system in danger. Governments, operators and service providers all express their concerns about cybersecurity, for example, integrity of products, no backdoors, security of their supply chains, and personal data protection.

Insisting on openness, transparency, and trust, ZTE implements its cybersecurity governance via a top-down approach. Based on a 'three lines of defense' security governance model, ZTE not only integrates its security policies into every phase of the product lifecycle, but also implements its cybersecurity assurance mechanism throughout a product lifecycle, thereby ensuring that product R&D, supply chain, production, engineering services, management of security incidents, independent verification and audits are all included. By developing cybersecurity baselines, underpinned by processes, and implementing closed-loop management for cybersecurity, ZTE enables end-to-end secure delivery of products and services.

<sup>1</sup> [https://enterprise.verizon.com/resources/reports/DBIR\\_2018\\_Report.pdf](https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf)

<sup>2</sup> <https://www.cvedetails.com/>



## Focus and Commitments from ZTE Leadership Team

ZTE attaches utmost importance to our customers' security values, abides by the relevant laws and regulations with respect to cybersecurity, and ensures end-to-end delivery of secure and trustworthy products and services. Cybersecurity is one of the highest priorities for ZTE's product development and delivery. We have established a holistic cybersecurity governance structure across the company's strategic development plan, taking into account relevant laws, regulations and standards, thereby fostering good security awareness for all employees and emphasizing the security of the entire process.



## Elements of ZTE's Cybersecurity Strategy

ZTE's end-to-end cybersecurity assurance program adheres to a six key elements: Standardization, Strict implementation, Traceability, Strong supervision, Full transparency, and Trustworthiness.

**Standardization:** The respect for global rules and standards, developed into a series of cybersecurity policies, standards, processes, and guidelines to help shape and drive the business.

**Strict implementation:** Cybersecurity within each business unit is strictly implemented in accordance with the regulations, supported by an accountability system and a "Product Security Red Line".

**Comprehensive supervision:** Improved supervision and management by implementing the three lines of defense security governance model.

**Traceability:** End-to-end product development activities supported by evidential records and traceability, ensuring that problems can be detected and located quickly.

**Full transparency:** Open up our processes and procedures to allow customers, governments, and other stakeholders to validate our cybersecurity. Customers can validate security activities on site. Security issues and vulnerabilities are disclosed in a transparent way. The patches are released timely.

**Trustworthy:** Win customers' trust through open and transparent security governance activities and third-party security verification and certification.



## A Three Lines of Defense Security Governance Model

Organizationally, ZTE implements a three lines of defense security governance model to ensure the security of the products and services from multiple perspectives. In the first line of defense, each business unit is responsible for implementing self-control over cybersecurity, using best practice processes and procedures. The company's Product Security Dept. is the second line of defense, responsible for independent security assessments and supervision. Finally, ZTE's Internal Control & Audit Dept. as the third line of defense checks and audits the effectiveness of the first and second lines of defense. At the same time, ZTE accepts the security audits organized by customers and external third parties.





## Developing Specialized Security Teams

ZTE organizes different types of security training to build security awareness and to grow professional security skills, these can take the form of, high-level seminars, management training classes, awareness training for all employees, secure design training, training on penetration testing, and secure coding competitions. Such training not only improves the security of the company's products, but also fosters a cybersecurity culture within the company.

ZTE attaches great importance to the cultivation of professional security talent. Currently, ZTE has more than 30 employees who have been certified by international organizations like CISSP, CISA, CSSLP, CEH, CCIE, CISAW, and C-CCSK for their security skills. ZTE shows sound security capabilities in terms of mature security architecture, secure design principles, comprehensive penetration testing, security audits, and security management.



## End-to-End Secure Delivery

The security of every single part of the system could impact the entire system. However, the strength of a whole system is determined by the weakest part. ZTE's security governance includes R&D, supply chain, engineering services, incident management, and all support functions. Take R&D for example, the security controls are included in the phases of security requirements, secure design, secure coding, security testing, secure delivery, and secure Operations and Maintenance (O&M). The security of third parties' components is taken into consideration too. Take Supply Chain for another example, the security activities are involving purchasing, production, manufacturing, warehousing, shipment, and final delivery.



## Response to Cybersecurity Incidents

ZTE's Product Security Incident Response Team (PSIRT) identifies and analyzes security incidents, tracks incident handling processes, and communicates closely with both internal and external stakeholders to disclose security vulnerabilities in a timely manner, thus ensuring that we mitigate the adverse effects of security incidents. As a member of the Forum of Incident Response and Security Teams (FIRST) and the CVE Numbering Authority (CNA), ZTE is collaborating with customers and stakeholders in a transparent manner to ensure we do all we can to protect our customers' networks.



## Independent Assessments and Verification

Under the three lines of defense security governance model, independent security assessments and verification belonging to the second line of defense are performed to evaluate and supervise the front-line security practices. Based on risk control principles, independent security assessments and verification review cybersecurity from multiple perspectives. A supervision and control mechanism is implemented to further reduce security risks. Closed-loop management is used to track identified problems and ensure they are resolved. All these measures ensure that ZTE's cybersecurity governance constantly keeps improving.



## Security Audits

---

ZTE's security audits independently evaluate the robustness, soundness, and effectiveness of our cybersecurity assurance system. The aspects to be audited include organization and operation, risk management processes, control activities, and internal supervision. The company's security audits cover the end-to-end cybersecurity assurance process, which includes general cybersecurity governance, R&D security, supply chain security, service delivery security, security incident response, and independent security assessments. The goal is to realize the supervision and transparency for the whole cybersecurity program.



## Third-Party Security Certification and Cooperation

---

In 2005, ZTE first passed the ISO27001 Information Security Management System (ISMS) certification. This certification needs to be reviewed every year and covers all ZTE business, with our latest certificate being awarded in 2018. In 2017, ZTE passed ISO 28000 Supply Chain Security Management System certification. To date, ZTE's 12 categories of products have passed Common Criteria (CC) certification (which is an international standard for product security certification). Products having been awarded CC certification include several mainstream products and equipment, for instances, equipment for core networks and access networks, optical transport equipment, network management equipment, router, and base station controller.

ZTE also actively cooperates with multiple third-party organizations to assess the company's cybersecurity. For example, the third parties are entrusted with source code audits, security design assessments, and penetration tests.

Based on ZTE's vision for cybersecurity, which is "Security in DNA, Trust through Transparency", ZTE's final objective is to provide our customers with trustworthy solutions and end-to-end security assurance throughout the entire lifecycle of a product. The company remains committed to communicating and cooperating with regulatory agencies, customers, partners and other stakeholders in an open and transparent manner to jointly create and improve a secure ecosystem for cybersecurity.

*This white paper sets out ZTE's strategy, vision, mission, objective, and tactics in terms of cybersecurity, introduces the company's end-to-end cybersecurity practices, including the building of its three lines of defense security governance model, security for R&D, Supply Chain, delivery, and information, security incident management, business continuity management, independent security assessment, and security audit. The paper concludes with an overview of ZTE's milestones in the field of cybersecurity.*

# ZTE's Cybersecurity Strategy





*Telecommunications networks are classified by countries as critical network infrastructure (CNI). All the services (including public services) running on these networks are seen as crucial to the normal functioning of a country. Operators, governments, and users place a high value on the security of telecommunication networks. ZTE also attaches great importance to the security of these CNI networks, and has formulated a cybersecurity strategy that ensures that security is one of the highest priorities in terms of R&D and delivery of the company's products.*

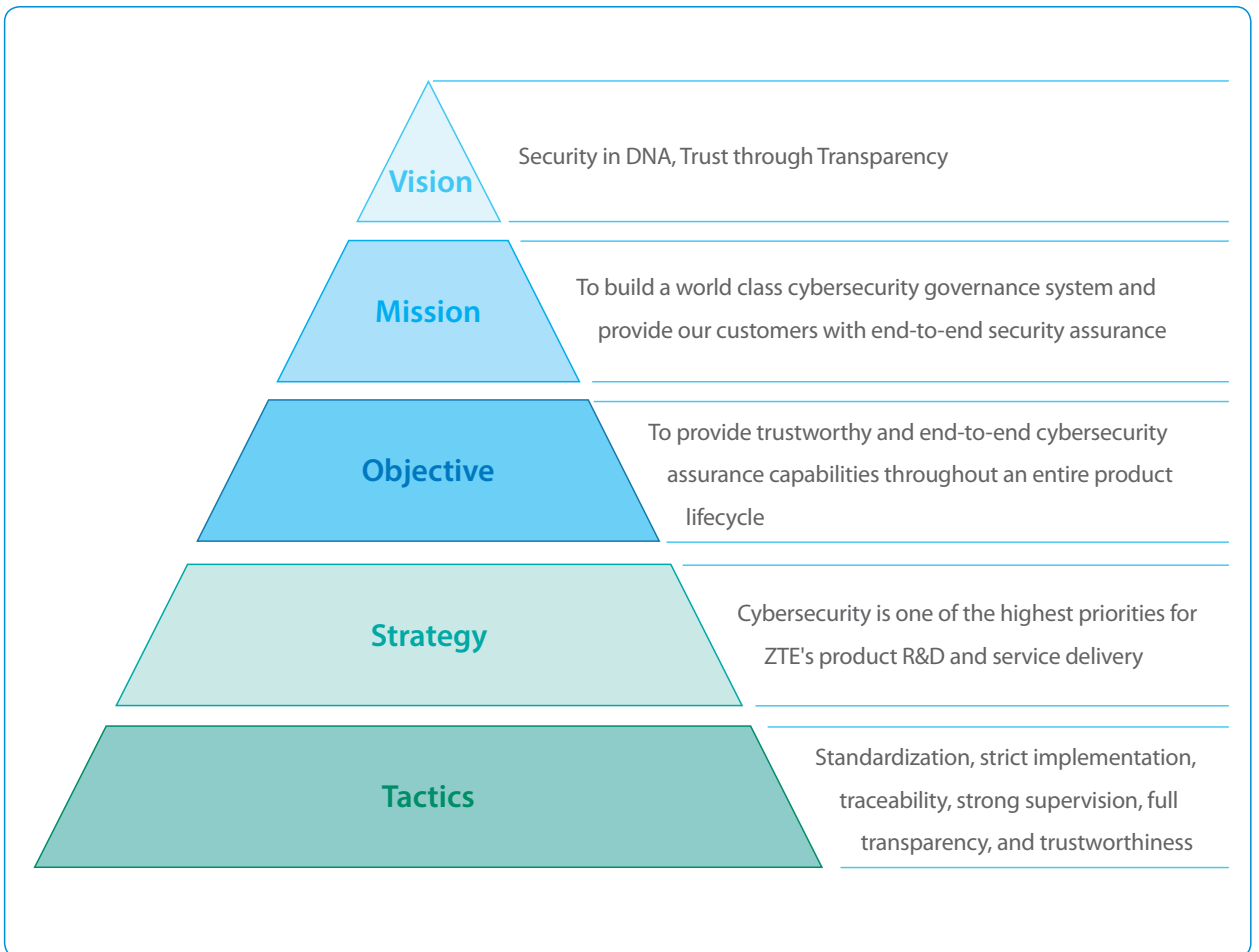


Figure 1 Cybersecurity Strategy



## **Vision: Security in DNA, Trust through Transparency**

---

Rather than being an additional feature, security is seen as an intrinsic property of our products. ZTE embeds cybersecurity in our business, organization, processes, technologies, and culture. ZTE is willing to share with customer details with respect to product fulfillment and process assurance. ZTE believes customer's trust is built through openness and transparency. ZTE will empower customers to check our products source code, and design documentation, get an overview of the operating systems, to carry out comprehensive testing, and to understand the security measures ZTE has taken in the development of our products.



## **Mission: to build a world class cybersecurity governance system and provide our customers with end-to-end security assurance**

---

ZTE Senior management are committed to continue investing resources into build a world class security governance system, which includes optimizing the organizational structure, human resources, processes and procedures, and innovative technologies to ensure that the company's business proceeds safely and customers get end-to-end security assurance.



## **Objective: to provide trustworthy and end-to-end cybersecurity assurance capabilities throughout an entire product lifecycle**

---

ZTE will provide secure end-to-end cybersecurity based on customers' requirements and expectation. In accordance with relevant laws and regulations, security standards, and principles of best practices, ZTE will guard networks, equipment, applications, and data against attacks, damage, and unauthorized access by providing end-to-end cybersecurity solutions through relevant organization, processes, and technologies.

ZTE is committed to building a sound cybersecurity governance structure and creating an end-to-end security assurance mechanism for all phases of the product lifecycle, for example, the product R&D, supply chain and manufacturing, engineering delivery, security incident management, assessment, and audit. By building a three lines of defense security governance model, establishing cybersecurity baselines, developing processes for security management, implementing closed-loop management for cybersecurity, and by providing reliable cybersecurity delivery capabilities, ZTE will build trust and ensure that our cybersecurity process is world class.

To improve customers' confidence in ZTE's cybersecurity capabilities, we will ensure product integrity checking, no backdoors, secure supply chain, and protection for personal data, to name but a few examples.



## Strategy: Cybersecurity is one of the highest priorities for product development and delivery

---

In ZTE, cybersecurity will always get top priority, irrespective of the required functions and or progress. With respect to the key decision-making points in R&D and engineering processes, ZTE gives top priority to cybersecurity in making any decision.



## Tactics: standardization, strict implementation, traceability, strong supervision, full transparency, and trustworthiness

---

**Standardization:** Respect rules and standards and develop world class cybersecurity polices and process specifications for every product and every process. Formulate a series of policies, standards, processes and procedures, and guidelines regarding cybersecurity.

**Strict implementation:** Measure and monitor the daily work of each business unit to ensure strict compliance in accordance with the recommended regulations. Strengthen the implementation by building an accountability system and releasing the "Product Security Red Line".

**Strong supervision:** Strengthen supervision and management through the three lines of defense security governance model. Ensure that the regulatory department implements process audits and checks the implementation status of the security standards, with audit results and the implementation status of the security standards being reported to the company's Cyber Security Committee.

**Traceability:** Ensure that the components and location of a product can be maintained and managed. All activities involving cybersecurity must be retrievable through records and traceable through evidence, allowing problems to be detected and located quickly.

**Full transparency:** Open up ZTE's end-to-end activities with respect to cybersecurity to customers, governments, and other stakeholders. Customers have access to activities such as code checking, full disclosure of any security problems, vulnerabilities, and patches in process. The establishment of an overseas security lab where customers can check systems, source code, and technical documentation of ZTE's products. As a CVE numbering authority, ZTE gives stakeholders access to its security handling processes for vulnerabilities through standard vulnerability exposure policies.

**Trustworthy:** Win customer trust through open and transparent cybersecurity governance activities and third-party security certification. ZTE sets up close partnership with customers, third parties, and regulatory agencies to carry out source code audits, security design review, and supplier audit all the time.

# End-to-End Cybersecurity Practices



“

ZTE meets the applicable cybersecurity laws and regulations, with respect to international and domestic standards, and is based on best in class security practices. ZTE researches security practices from leading enterprises, in order to continuously improve our own security practices, while constantly strengthening our cybersecurity capabilities, to provide customers with secure and trustworthy products and services.

”

## Cybersecurity Governance Architecture Based on Three Lines of Defense

ZTE has set up an organizational architecture based on three lines of defense to promote cybersecurity governance. This structure solves conflicts of interest by using the organizational mechanisms, and avoids the risks of front-line business units sacrificing security requirements for market progress, driven by demand for products and services. The structure also follows the principle of risk control, by guaranteeing cybersecurity from multiple perspectives and multiple levels through self-inspection by business units, the independent security assessment of the second line of defense, and the security audit of the third line of defense.

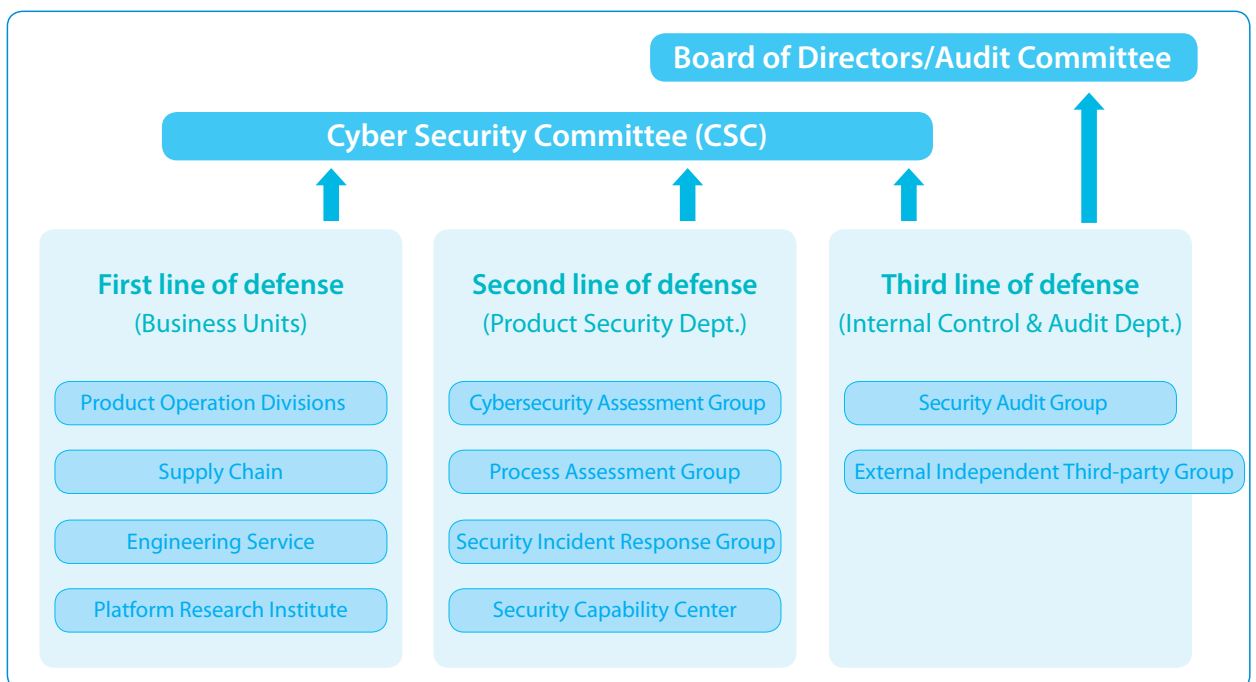


Figure 2 Cybersecurity Governance Architecture Based on Three Lines of Defense





## Board of Directors/Audit Committee

---

The Board of Directors authorizes the Cyber Security Committee (CSC) to carry out cybersecurity governance work. The Board of Directors or the Audit Committee also reviews the security audit reports provided by the Internal Control & Audit Dept. This ensures that ZTE products and solutions receive the highest level of commitment at board level.

## Cyber Security Committee (CSC)

---

The lead decision-making organization responsible for the cybersecurity work of ZTE. The Cyber Security Committee formulates cybersecurity strategies and guarantees resources, determines the strategic direction and objective of the cybersecurity work, reviews cybersecurity plans, and decides major issues related to cybersecurity.

## First Line of Defense (Business Units)

---

Each business unit is the first line of defense for cybersecurity governance. Each business unit realizes the self-control of cybersecurity through the processes and procedures approved by the CSC for self-planning, self-execution, self-detection and self-improvement of cybersecurity.

## Second Line of Defense (Product Security Dept.)

---

The Product Security Dept. is the second line of defense for cybersecurity governance. As a permanent member of the CSC, the Product Security Dept. is responsible for promoting the implementation of all management and technical practices related to cybersecurity, coordinating the construction of cybersecurity policies and procedures, guiding the business, inspecting security implementation, supervising and evaluating the progress of the first line of defense.

## Third Line of Defense (Internal Control & Audit Dept.)

---

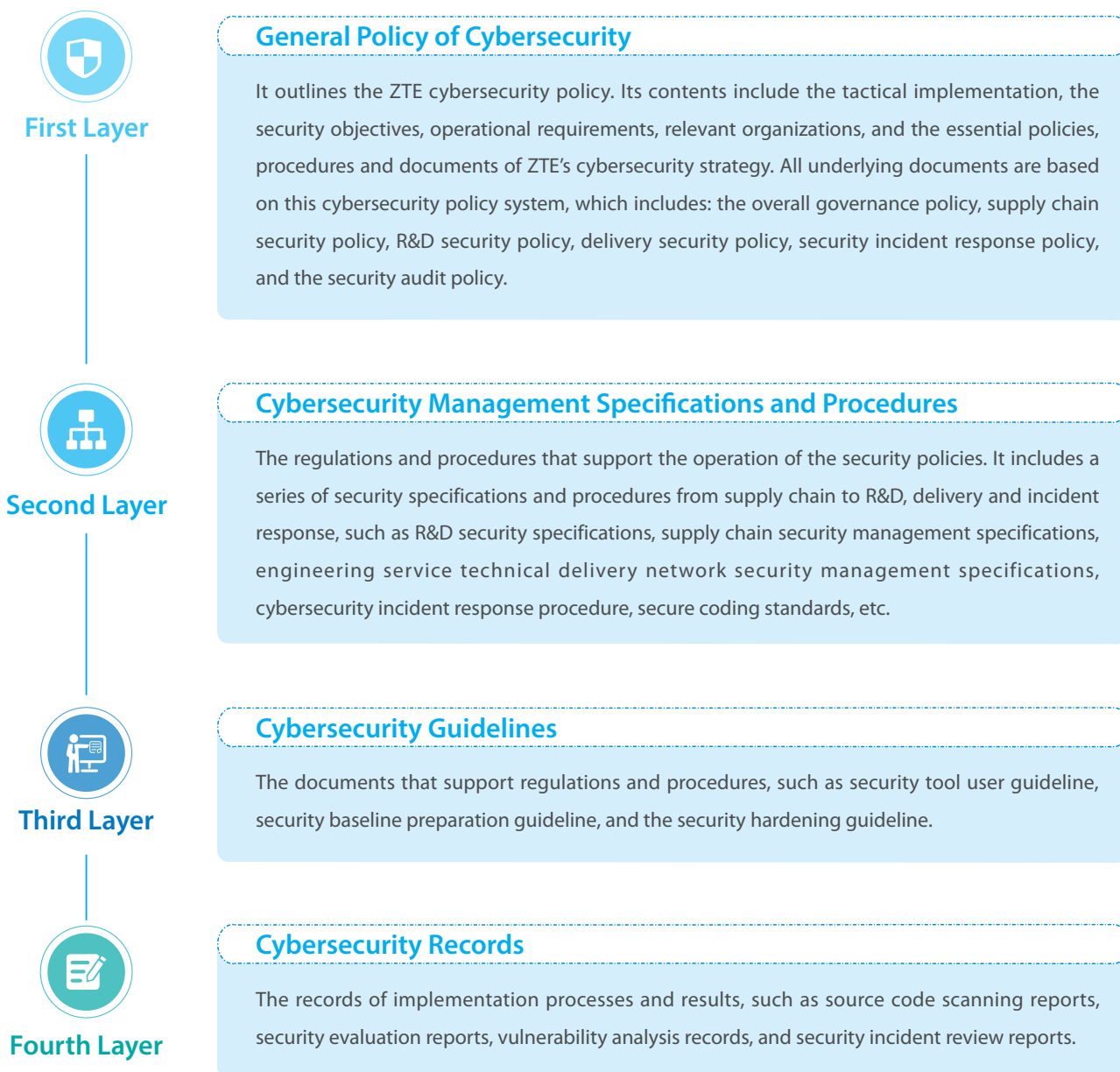
The Internal Control & Audit Dept. is the third line of defense for monitoring and evaluating cybersecurity governance. The Internal Control & Audit Dept. is responsible for auditing the first and second lines of defense, including the conformity check and cybersecurity testing of the procedure implementation, and reporting the audit results to the Board of Directors/Audit Committee. The Internal Control & Audit Dept. can jointly audit the cybersecurity implementation of ZTE with external third-party auditors.

Cybersecurity governance also involves other support teams such as Human Resources, Finance and Accounting, Strategy and Investment, Operations Management, Public Affairs, Legal and Compliance, and Administrative Affairs and Real Estates.

# Cybersecurity Specification System

ZTE has established robust cybersecurity policies, standards, procedures and guidelines. The cybersecurity policy system recommends a comprehensive set of requirements for cybersecurity governance. ZTE has issued a series of security management specifications and standards, which are under regular review. Each business unit carries out the practical security activities in accordance with these cybersecurity requirements. During the practical implementation of the security specifications, corresponding results and records are captured, which are available as evidence to relevant parties for auditing.

The ZTE cybersecurity document system is divided into four layers.



# R&D Security

Security is one of the highest priorities in ZTE's product R&D and service delivery activities. While pursuing efficient R&D, ZTE pays significant attention to product security and incorporates "security" into the product development life cycle as a basic attribute of the product, ensuring that ZTE has reliable product security delivery capabilities that customers can rely on, providing customers with secure products and solutions.

## R&D Security Procedures and Organizations

The High Performance Product Development (HPPD) process is a common procedure guiding R&D within ZTE. The process is subject to continuous improvement and is regularly evolved to meet the requirements of customers and market conditions. Security is a basic element of the product development process and is integrated into the HPPD process, thereby ensuring that security is developed into all our products, even at the early concept stage.

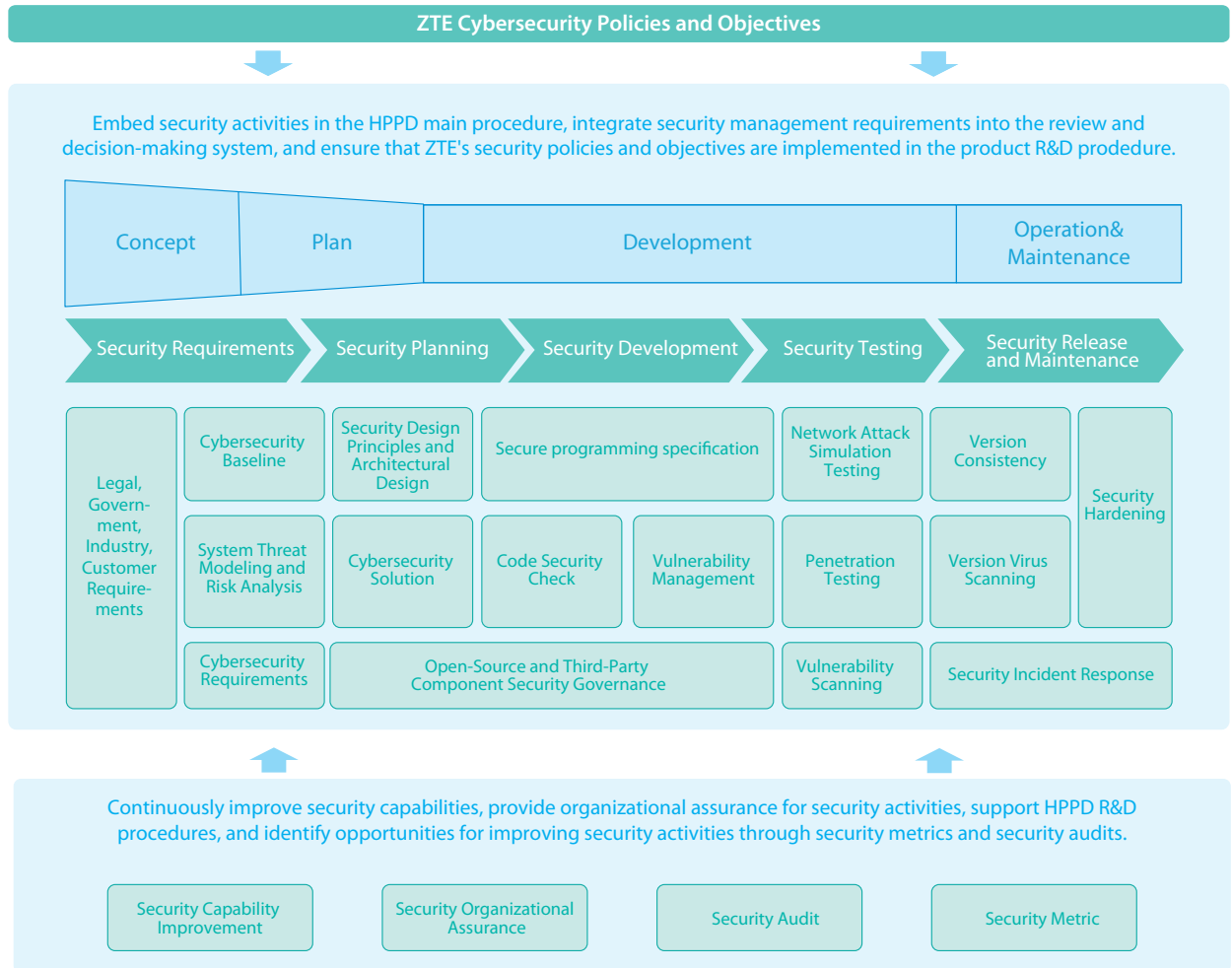
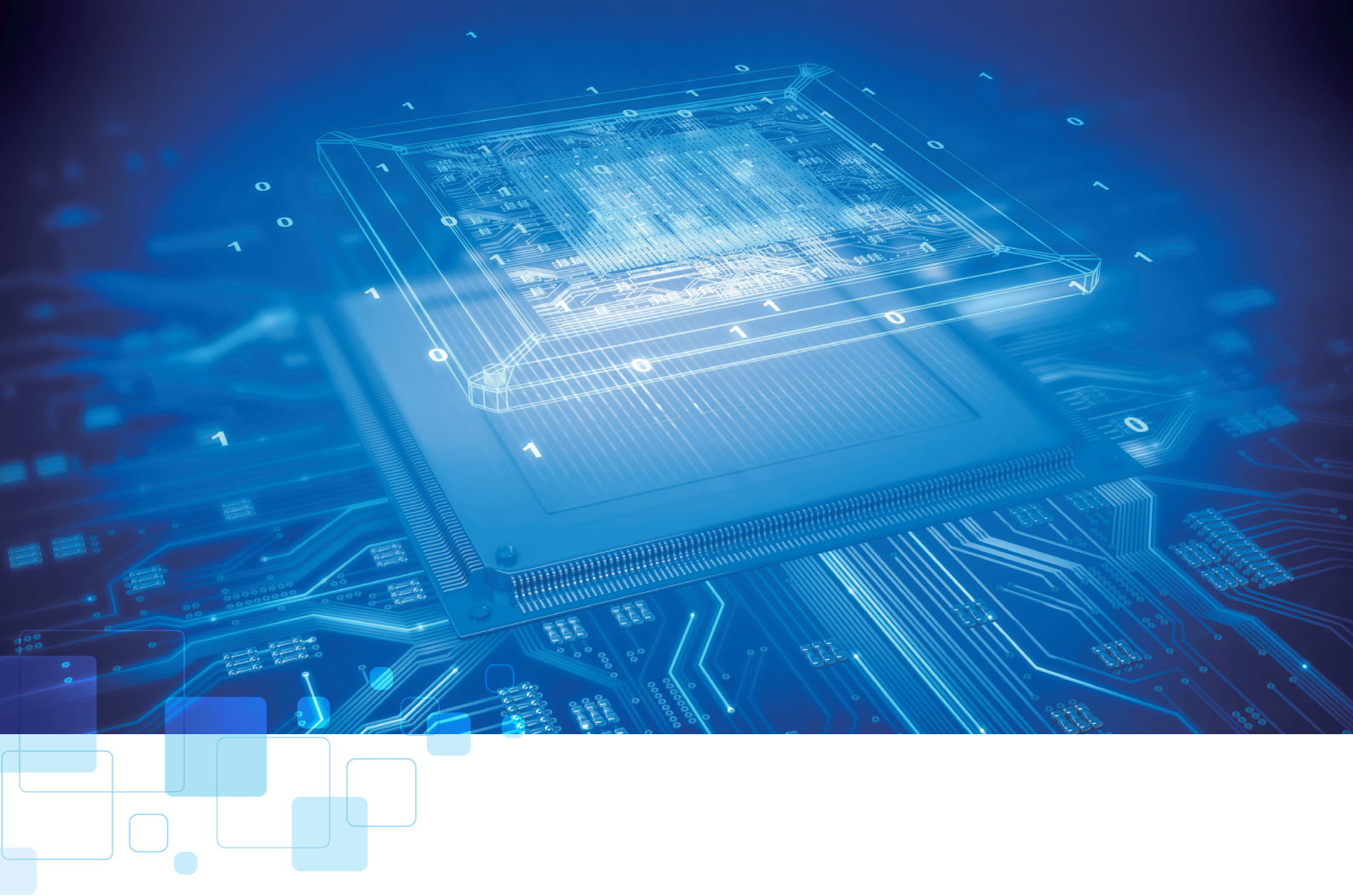


Figure 3 Security Activities Embedded in the HPPD Main Process



ZTE combines R&D activities with reference to industry security practice models such as BSIMM<sup>3</sup> and Microsoft SDL<sup>4</sup> to define security activities such as security requirements, security planning, security development, security testing, security delivery and maintenance in the HPPD process, to ensure that security features are effectively integrated into our products. At the same time, ZTE continuously improves its security capabilities and provides organizational assurance for security activities, thereby effectively supporting the operation of the HPPD process. ZTE also implements security audits and security metrics to continuously improve the HPPD process.

The HPPD process is embedded into the product development process with comprehensive security elements to ensure the effective implementation of security activities. In order to provide more secure products and solutions to customers, the security requirements are integrated in the end-to-end business procedure, such as security threat analysis in the requirement analysis, security architecture design in the product design, secure coding and source code security scanning in the product development, security function testing and penetration testing in the product test, vulnerability scanning in the product release, and version consistency guarantee, etc.

In terms of product R&D security organization guarantee, ZTE has set up a Software Security Group (SSG) with the cybersecurity directors as its core member. The backbone staff of the major teams involved in the end-to-end development of products, such as planning, R&D (requirement, design, development, and testing), supply chain, delivery, and market, all use a common threat model to understand the security requirements, and to ensure that risks in all fields involved in the products are fully identified and the problems are quickly resolved. The company-level CSC makes decisions on major risks and problems related to cybersecurity, and authorizes the SSG supervisor to provide business guidance to the cybersecurity director.

<sup>3</sup> <https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html>

<sup>4</sup> <https://www.microsoft.com/en-us/securityengineering/sdl/>

## Concept Phase

During the concept development phase, ZTE incorporates strategic medium and long-term security requirements into the product roadmap planning, while ensuring that well known short-term security requirements are incorporated into the product version roadmap. Short-term planning typically includes planning, according to the current market admission requirements (laws, regulations and industry standards), customer security requirements, competition analysis, industry activities, peer experience, specific information protection, and internal security requirements.

ZTE's cybersecurity requirements consist of two parts: one is ZTE's cybersecurity baseline, which is enforced as the most basic security requirements. The second is to assess the risks of the application scenarios of the products in the operator networks or the government and enterprise networks, and to incorporate relevant countermeasures into the security requirements.

## Plan Phase

In the planning phase, ZTE has developed a product security design specification with reference to the security specifications and industry best practices, such as ITU-T X.805, ISO 15408, 3GPP and IETF. During this phase, the R&D team further refines the security requirements and designs the security architecture and feature security of the products based on the cybersecurity design specifications.

ZTE analyzes the security requirements and potential security threats of the system, determines the security architecture and the system solution of the products, and then ensures that the system solution meets the security requirements of the market and our customers. According to the ZTE security admission standard, a professional team will verify the security of our suppliers' products and solutions, and also evaluates the security of third-party components.

ZTE understands security requirements through threat modeling. A set of system threat modeling methods for communication products called SATRC<sup>5</sup> is utilized, and is based on industry best practices such as ITU-T X.805, Microsoft STRIDE/DREAD, Synopsys ARA and other models. This model ensures that ZTE is able to



### Define the System

Decomposes the business scenario, establishes the system logic architecture model, identifies the trust boundary and entry point, and draw the data flow diagram;



### Identifies the Assets

Hardware, software, data, and service;



### Discovers the Threats

Completes the model and outputs the attack list;



### Evaluates the Risks

Evaluates the threats according to the risks caused by the threats;



### Develops the Recommended Control Measures

By determining the corresponding countermeasures against the threats according to the level of the risks.

<sup>5</sup> SATRC: System, Asset, Threat, Risk, Control



## Development Phase

In the development phase, code implementation and security document are developed and completed in accordance with the requirements of the secure coding specification, and the code is then checked statically and scanned automatically.

### Secure Coding and Code Security Check

Based on the industry's authoritative secure coding specifications, such as CERT (Computer Emergency Response Team), OWASP (Open Web Application Security Project), CWE (Common Weakness Enumeration), and STIG (Security Technical Implementation Guide), ZTE established the C/C++/Java/Web secure coding specifications. ZTE also operates industry-leading source code scanning tools such as Klocwork, and Coverity. ZTE effectively detects and identifies the quality, reliability, security vulnerabilities and maintainability of the various elements of the code that make up products. ZTE also implements effective tracking and management measures for problems detected by the tools, such as the Kanban management of Klocwork data, which monitors the remaining defects over time.

ZTE has established a three-layer inspection control-point mechanism that scans the source code three times, namely: individual building self-test, module building scan, and project building scan. ZTE produced code cannot pass through the next control gate if the goal of zero security defect is not met as part of the HPPD process.

## Testing Phase

ZTE develops security testing procedures and solutions, designs and executes testing cases to verify the security function modules, performs vulnerability scanning, protocol robustness scanning, penetration testing on products, and completes a system vulnerability analysis. ZTE determines the security hardening implementation solution of products, and provides the evidence required for cybersecurity certification.

## Release Phase

ZTE products are only guaranteed for release after being checked with multiple mainstream anti-virus software solutions for zero anomalies. At the same time, from the version release to the user for deployment, as including the operation and maintenance process, all necessary security protection is carried out to ensure the consistency of the released version.

The software version is protected by obfuscating tools, such as renaming, string encryption, virtual code insertion, and code logic obfuscation, which make it difficult for an attacker to obtain the original code directly by using reverse engineering tools, thereby strengthening the protection of ZTE products.



## Third-Party Component Security Governance

ZTE implements full life cycle management of any third-party components required, from the introduction of these third-party components to their delivery to the customer as part of the product. ZTE embeds comprehensive security risk assessment, security testing, and vulnerability management of third-party components into the HPPD process. This ensures that once a security vulnerability is discovered during the product life cycle, the vulnerability is evaluated, and a solution or circumvention is provided to PSIRT to quickly resolve all the problems related to the third-party components.

ZTE has established an area to store all third-party components, and strictly controls the use of the third-party components. This ensures that developers can only obtain components from certified sources, and centrally ensures that the third-party components are compliant, secure and up-to-date. ZTE uses third-party components as configuration items in the software configuration management procedure to ensure that the use of components can be traced.

ZTE joined the open source community, and continues to track vulnerabilities released by the community, while actively submitting security vulnerability solutions. ZTE also actively contributes to the security of open source components.

## Continuous Security Delivery

The continuous security delivery of DevSecOps (Development Security and Operation) is guaranteed by a robust configuration management support system and a DevOps (Development and Operation) toolchain integrated with the development procedure.

ZTE's configuration management system ensures traceability for the customer's original requirements along all phases of the procedures, from design, software coding, testing, quality assurance, existing network deployment, and for the faults found on the network to the original source, from the customer's original requirements to the final product, and from the final product to the original requirements - covering all steps, all processes, all the people who have been involved in the software development process, all the components, and all the software version numbers.

At the same time, ZTE integrates the security tools into the entire DevOps toolchain. Through continuous planning, collaborative development, continuous testing, release and deployment, the four links are iteratively connected in series. In key activities such as code scanning, security testing, vulnerability scanning, and version protection, the security tools are guaranteed to be used efficiently to form an O&M monitoring closed loop.

ZTE identifies the information security risks of the code and determines the control measures. The R&D personnel access the desktop cloud through the terminal, and access the R&D cloud. The code are compiled, unit/function tested and reviewed in the R&D cloud to form the delivery version. ZTE also develops a response control policy for the flow of code and documents between the desktop cloud and the R&D cloud. For example, the code cannot be copied out of the cloud without approval; the entities in the whitelist can access the Internet from the desktop cloud, but the Internet cannot be accessed from the R&D cloud; the personal terminals can access the Internet but cannot access R&D cloud and IT service resources; the external community development can be joined through the transfer code library; level-A regional control is performed in debugging areas to ensure that the code are securely controlled during the development process.

# Supply Chain Security

With the highest levels of openness across the globe, the information technology industry features a globally distributed industry chain, with communications equipment providers inevitably requiring the support from business partners in the global industry chain. Components from any third party could pose security risks, ZTE Corporation has therefore implemented a series of monitoring measures in the business operations of the supplier and material management, manufacturing and return-for-repair, logistics and warehousing chain that might contain cybersecurity risks, to ensure no security faults are introduced, generated or spread in these business activities, and to securely deliver the self-developed products and auxiliary materials purchased from third parties to our customers.

ZTE integrates cybersecurity requirements into the business processes of the supply chain, including the supplier and material management process, manufacture and return-for-repair process, and logistics, warehousing and reverse logistics processes.

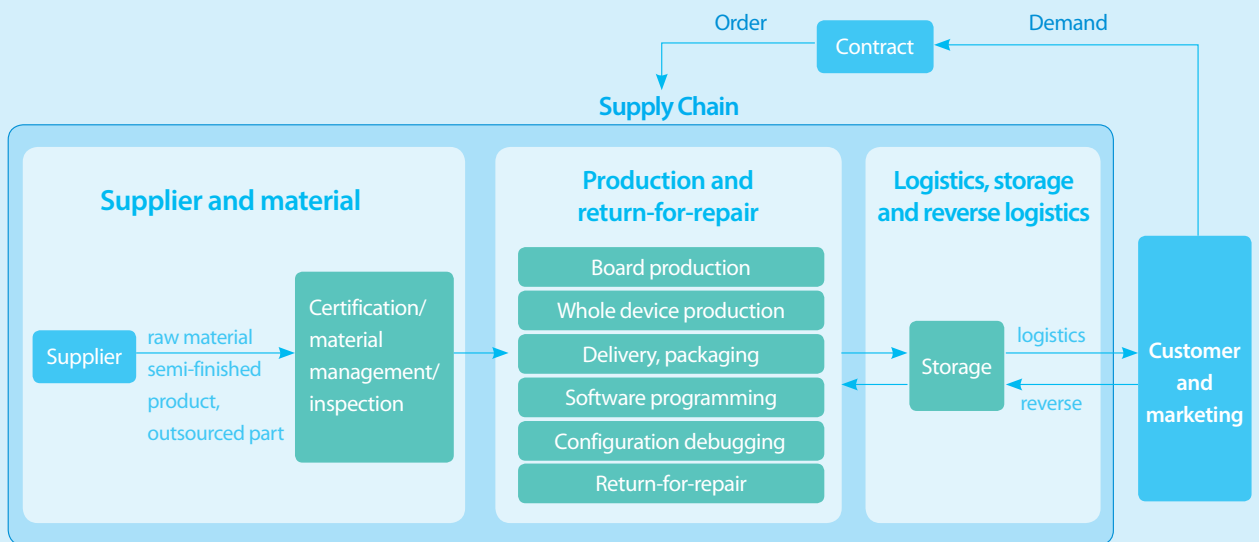


Figure 4 Process Chart of Global Supply Chain Management

A special security assurance team has been established to identify any cybersecurity risks within the supply chain, to refine the business process, and to work out effective risk control measures and response schemes for security incidents. In addition, constant improvements are being made to ensure that the cybersecurity control measures are properly implemented, and to guarantee the integrity, reliability and traceability of the company products across the supply chain.

ZTE Corporation has passed ISO 9001 certification, and has also joined the Quality Excellence for Suppliers of Telecommunications Forum (QuEST Forum) and now serves as co-chair for the Asia-Pacific and greater China regions. In 2017, ZTE Corporation was officially certified with ISO28000 (specification for security management systems for supply chain) and the Customs AEO Trade Security, which marks a new milestone achieved by the company in terms of the supply chain security management.



## Supplier and Material Management

ZTE Corporation is dedicated to building a long-term stable relationship with our business partners. By implementing strategic procurement processes and constantly exploiting cooperation opportunities with strategic partners, we have formed a win-win relationship building upon mutual trust, stability and sustainable development. Meanwhile we expect that our business partners will engage in early product R&D and market projects to create more value.

ZTE has established the Communities of Practice (COP) forum, which has enabled a brand-new channel for technology exchange and cybersecurity communication with our business partners. It is a learning environment where formal and informal learning are mixed. Ever since the establishment of the Materials COP in 2017, ZTE has held over one hundred on-line and off-line technology exchanges together with multiple suppliers. In addition, we have hosted CTO Day activities with many business partners in 2018, which has been proved to be a great success.

The implementation of strategic procurement is not only reflected in the point-to-point collaboration between ZTE and individual suppliers. We also look forward to making joint efforts with more upstream and downstream partners to build an ecosystem. In this way, we hope to expand the industry chain by galvanizing innovation and practice on standard, technology, product, market and business models, and to form a closer strategic alliance through joint planning, IT system integration, exchanging managerial experience, drawing upon each other's advantages, and making improvements together across the supply chain. In the thriving industries of 5G, Internet of Things, big data and artificial intelligence, we will continue to enhance cooperation with our business partners.

Supplier and material management is a key part of the company's cybersecurity management system. Thousands of suppliers and business partners located all over the globe, that collaboratively provide tens of thousands of raw materials, semi-finished products, finished products or services for ZTE, are a key part of the products and the integrated solutions that we provide to our customers.

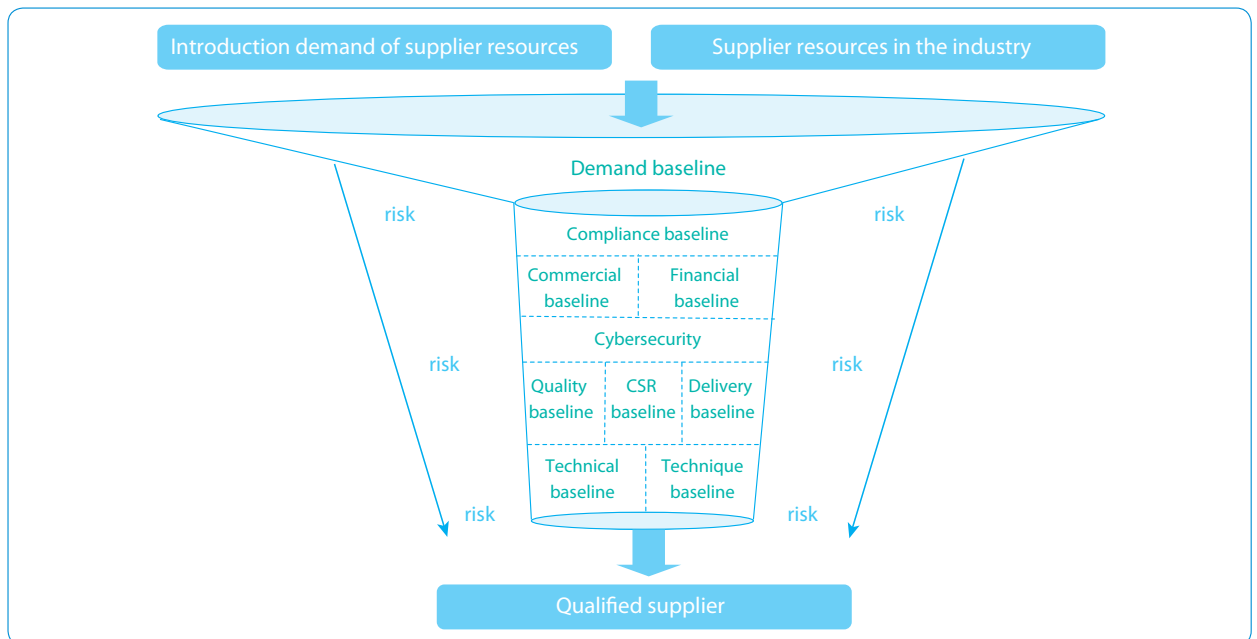


Figure 5 - Suppliers Admission System of ZTE



ZTE has always attached great importance to the establishment of a supplier management system, and have established a comprehensive set of management processes and procedures for supplier life cycle management, from sourcing assessment, product certification, to end of market supply, including cybersecurity management, supplier social responsibility (CSR) management, quality management, performance appraisal, and problem-tracing. A potential supplier can become one of the qualified suppliers for ZTE, only after passing a comprehensive evaluation on cybersecurity and multiple assessments in other aspects.

In terms of materials management, ZTE has also developed a complete set of business management procedures. ZTE defines the cybersecurity risks of materials into three levels: high, medium and low. Cybersecurity testing of high-risk materials are conducted when new materials are introduced and when old materials are changed. For materials with medium and low risks, we require suppliers to conduct self-management and control by signing cybersecurity agreements. ZTE conducts security audits in a scheduled and unscheduled manner on the suppliers' implementation to the agreements.

Supplier's response to a cybersecurity incident is a key part of ZTE's response to the cybersecurity incident and is potentially customer affecting. ZTE requires that suppliers must provide products and services in compliance with the cybersecurity agreements, and issue vulnerability precautions and solutions in time, in order to minimize the security risks of outsourced products. In case security vulnerabilities are found in the process of security testing or use of products, suppliers need to work collaboratively with ZTE in tracing and locating the problem, and provide solutions with software patches, upgrades, replacement or recall of faulty materials in a timely manner.

## Production Security and Return-for-repair Security

Cybersecurity management during production is a key part of our company's cybersecurity management system. Based on the security management system for supply chain specification, ZTE has established a set of end-to-end management and control system for manufacturing security, which covers the entire process from incoming material inspection, component manufacturing, final assembly, to finished product packaging and warehousing, including a series of procedure documents, operation guidelines and other work instructions, which integrates the cybersecurity specifications requirements into the manufacturing operations. Cybersecurity standards requirements are integrated into awareness training and learning for employees.

In order to control the cybersecurity risks in production, ZTE has established an end-to-end management process to prevent software and hardware from being tampered with, which includes unauthorized hardware replacement, software insertion or tampering, and virus infection. In the production process, ZTE has identified several key procedures related to cybersecurity, including software version management, chip programming, final test of printed circuit board assembly (PCBA), module debugging, aging test, whole device debugging, packaging, return-for-repair, etc. According to the risk levels of cybersecurity, ZTE categorizes all the manufacturing and warehousing areas into three different levels of cybersecurity control areas, of which the level I and level II areas are the strictly managed areas. Security administrators are appointed in all the strictly managed areas to implement routine supervision and other security control measures. In addition, with the premise of compliance with applicable laws and regulations, ZTE also conducts a routine background investigation on the personnel in sensitive positions related to cybersecurity, to avoid any cybersecurity risk that may be caused by human factors. In the cybersecurity management process, ZTE engineers can archive and release software only through the Product Data Management (PDM) system that they are authorized to access, in order to protect software from being tampered with during manufacturing.

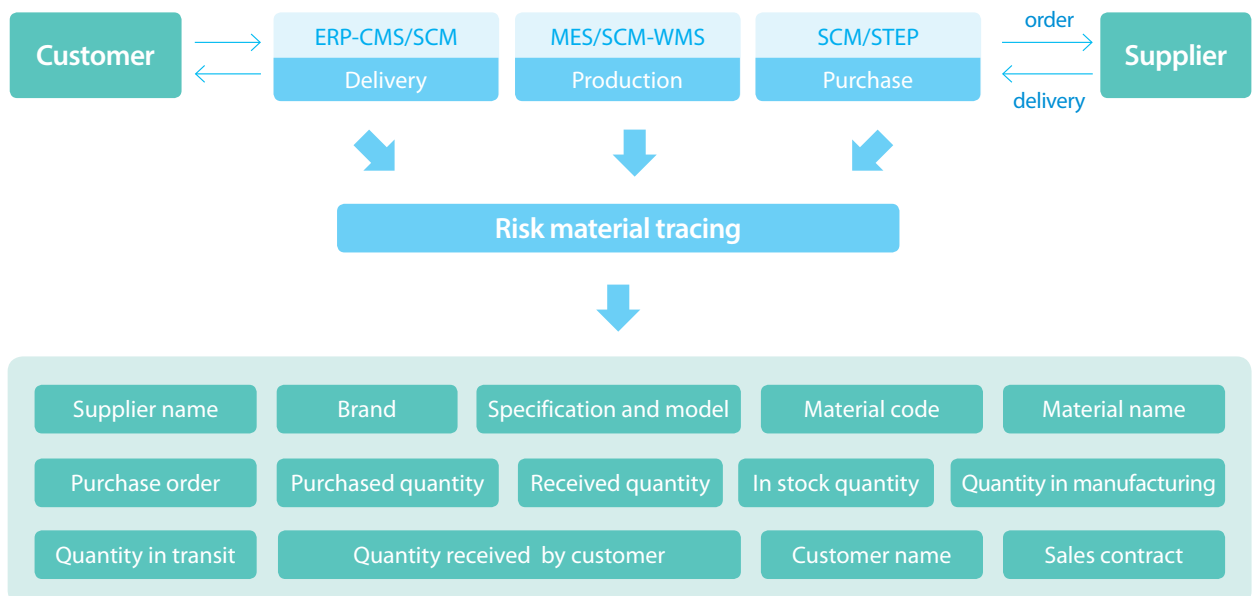



Figure 6 Management Process of Cybersecurity in Production



ZTE adopts the Manufacturing Execution System (MES) to record complete information of the manufacturing process. It enables effective end-to-end tracking of the product manufacturing process information according to the product bar code, and batch information. The incoming material lot numbers (sequence numbers) of supplier's products and components can also be traced. Meanwhile with the collaborative use of the Supply Chain Management (SCM) system for purchase, and Warehousing Management System (WMS) for delivery, MES enables an end-to-end management and tracking process from material purchase to product delivery. Using these management measures, ZTE can locate the very device, part, board or component that has quality problems or security vulnerabilities, and obtain the quantity and status of products that are in stock, in manufacturing, in transit, or received by customers to improve the efficiency in security incidents response.

Cybersecurity in the return-for-repair operation is a key part of cybersecurity management for ZTE. When defective products are returned for repair, ZTE reminds customer to process sensitive information through the Return Material Authorization Request (RMA) process or in other ways, such as data archiving, eliminating or removing the mobile storage medium, before returning the items for repair. In addition, after the equipment holding is transferred to ZTE, we shall guarantee the security protection of the software and hardware products of the equipment.

In the repair process, ZTE only uses materials from qualified and certified suppliers. It is prohibited to use any material or component from unknown sources, to ensure the equipment returned for repair is free from being compromised. Corresponding measures are also taken during the material and equipment recycle period such as video recording and network isolation, to ensure the equipment returned for repair is free from any illegal tampering, virus infection or data breach. ZTE has special processes and requirements for erasing data in the repair step. Equipment beyond repair and replacement will be collected and processed by a special unit. The return-for-repair of equipment is operated on the ECC-ASM system where data of the entire repair process is recorded for tracing, and one can learn about the status and the handler of the repair. The system has complete functions for search, record and information analysis.

## Warehousing and Logistics Security

In terms of logistics and warehousing, based on six domestic logistics centers and in collaboration with global logistics service providers, ZTE is building a national logistics center system, step by step, improving the performance of the global supply chain network, and planning elite freight routes to ensure timely project delivery. Through joint efforts with worldwide high-quality logistics service providers, based on the IoT technology and an intelligent platform, ZTE has implemented whole-process visualization of logistics status, ensuring the physical security of customer assets. ZTE has whole-process tracking of goods in warehouse through the Warehousing Management System. ZTE regularly upgrades the logistics & warehousing IT system, monitoring devices, and security facilities to avoid malicious code insertion and replacement or damage of core components during logistics and warehousing procedures. One-click query of order information and whole-process visualization of status are implemented through a visualization platform.

The complete management process of reverse logistics established in ZTE has made reverse logistics schemes possible in accordance with laws and regulations of local countries and regions, to meet the requirements for information security and privacy protection of customers and the local countries and regions where customers are located. In case the reversely returned equipment might contain sensitive data, ZTE will remind and request the customers to erase the data before returning it for repair. If a product is to be scrapped, a destruction report shall be required from the recycling dealer. Sensitive products should be scrapped under on-site supervision by specially-assigned staff.

# Delivery Security

Protecting the security of products delivered to our customers is our goal in delivery. ZTE uses both technical and management measures to guarantee secure delivery: On the one hand, secure products and services are delivered to customers as expected. On the other hand, all on-site personnel are requested to follow the codes of conduct related to delivery.

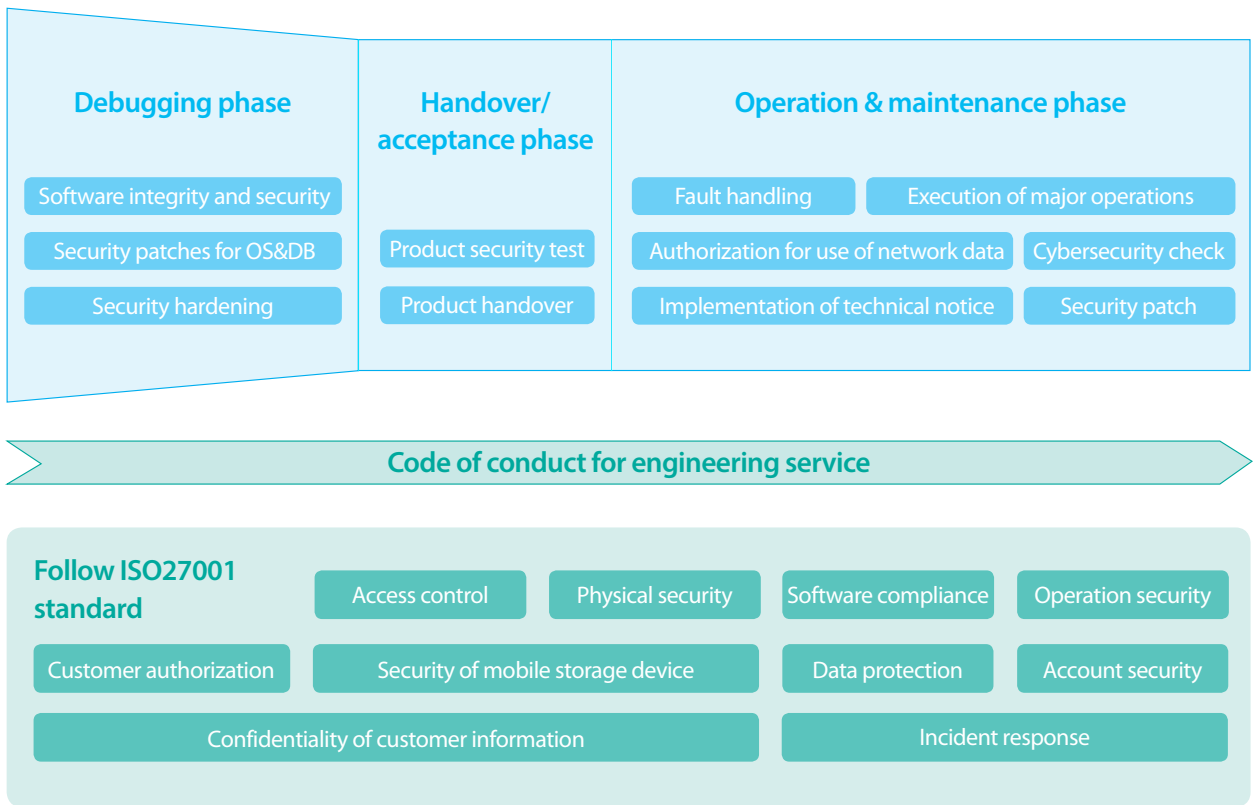


Figure 7 Security Measures for Delivery

A complete project delivery cycle covers three phases: debugging, handover/acceptance, and operation & maintenance. Key security check points are set in each phase. In accordance with the service characteristics in each phase, a series of security measures are defined in the delivery field to reduce possible risks that are caused by non-standard operation. Potential security risks are discovered and eliminated in a timely manner by using verifiable and repeatable security flows, regulations, and methods in accordance with consistent cyber security standards. ZTE has formulated the codes of conduct for the delivery field according to global laws and regulations, customer requirements and best practices (for example, ISO27001 Standard), to ensure the security of products and services delivered to our customers.



## Three Phases of Delivery Security



### Debugging Phase

---

In the debugging phase, verification measures are strictly implemented in the products delivery field to prevent the configuration from accidental modification. Software is downloaded only from a specified website. In addition, software consistency checks must be carried out before installation to ensure software integrity.

During the engineering commissioning and debugging period, on-site personnel take a series of actions such as detecting malicious programs through technical measures, installing designated operating systems or database patches, conducting vulnerability scanning, and completing hardening configurations in accordance with the guidelines to product compliance configuration and product security hardening.



### Handover/Acceptance Phase

---

Before a project handover, a series of security tests (with temporary configurations removed) are carried out to guarantee the security of products and test reports are output. Products can be handed over to customers only after going through the acceptance procedure. Besides physical equipment, the assets officially handed over to customers also include complete test reports and documents. The security of system accounts and passwords will also be guaranteed.



### Operation & Maintenance Phase

---

Security risks vary with new and emerging threats, laws and regulations, attack patterns, and vulnerabilities, ZTE delivery personnel continuously monitor the changes in the operation and maintenance phase to prevent the disclosure and tampering of data in the return-of-repair process, by conducting regular security checks and installing vulnerability patches in a timely manner. All operations are authorized by customers.



# Information Security

Information security is used to protect the security of the company's assets so that product R&D, production, and operation can be carried out in a secure environment. By establishing a comprehensive information security management system, control measures can be defined in terms of organization, personnel, procedure, and technology to ensure the confidentiality, integrity, and availability of data and assets, improved information security levels, and safeguarding of the business development of the company.

ZTE has established an Information Security Management System (ISMS) where the management processes of Information Security General Policy, Security Policy, Information Classification, Risk Assessment, and Security Audit are defined, and is supported by information security red lines. The information security organization shall monitor the red lines to supervise, investigate, and tackle any violations of the company's information security, and infringements on the company's business secrets. Each year, all employees will receive security training and be tested to raise and maintain their security awareness. The company has built several security reporting channels. For example, when dealing with information security breaches and exceptions, like risk and vulnerability exposure, employees can report them via the following channels, e-mail, phone, and the company's official website, while also being encouraged to handle the exceptions, fix the vulnerabilities, and complete the security rules in a timely manner.

ZTE has adopted a series of initiatives with respect to information classification, personnel security, physical security, and IT security to guarantee the security of the company's information assets, and ensure the confidentiality, integrity, and availability of information assets, while improving the information security level as a core competency of the company.

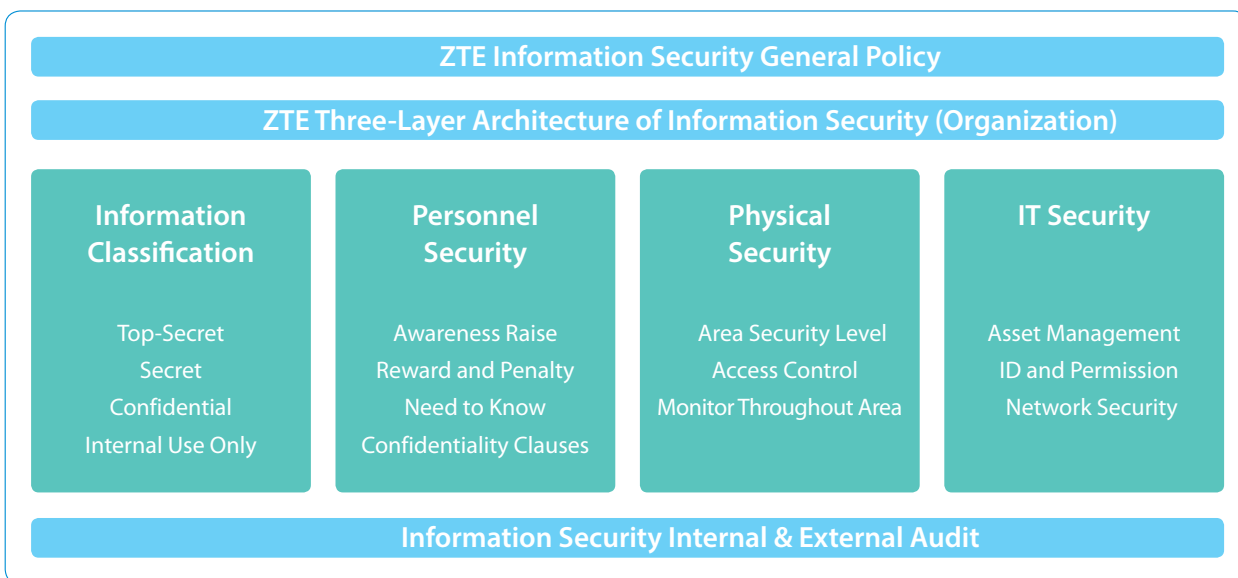


Figure 8 Overall Framework of Information Security



## Information Classification

ZTE has classified the importance of company information into four levels.

- **Top secret:** refers to top secret information, a breach of which will cause significant damage to the company's interests.
- **Secret:** refers to very secret information, a breach of which will cause strong damage to the company's interests.
- **Confidential:** refers to secret information, a breach of which will cause damage to the company's interests.
- **Internal use only:** refers to the information all employees need to be informed of, but not suitable for the public consumption.

ZTE has also formulated corresponding control measures for each level of information. ZTE protects customer information by classifying their data in a similar manner, with most customer information being classified into the secret or confidential level.

## Personnel Security

Personnel security is of equal importance as security awareness and behavior of employees play a vital role in a sequence of end-to-end activities like product R&D, manufacture, and delivery. ZTE maintains a control policy on personnel security during an entire product life cycle. For a personal position at a special level, with the premise of compliance with applicable laws and regulations, ZTE will entrust a third-party company to perform background checks and investigate the candidate. There are contractual confidentiality clauses stipulated in a ZTE labor contract, informing the employees about performing their duties in a confidential and responsible manner. Employees are also required to attend security training during new staff orientation. During their employment, employees need to sign ZTE's Information Security Commitment and will receive information security training and an examination at least once a year. When employees resign, they are required to sign the Information Security Statement for Employee Resignation and commit not to take any company information. Meanwhile, the employees, depending on their positions, shall be disengaged from secret information or comply with the Non-Competition Agreement.

## Physical Security

Depending on the level of secrecy a department in a region is classified to, ZTE has physically divided the security levels of areas based on the following classification scheme, A-level core secret area, B-level important secret area, C-level general secret area, and D-level public area. When employees enter into company, they need to present their staff ID for authentication. Any visit to company property must be documented by the receptionist in advance prior the visitor arriving. Security personnel can only allow a visitor access after verifying his or her identity. Core areas in the company defined at A or B level are equipped with separate physical controls, such as door access control systems, a security gate, or security personnel. Throughout the region, 24/7 security patrols and management are conducted and monitors are installed for added security. For example, the R&D debugging area and the security lab are managed using A-level controls to ensure that code security is maintained during its development. Moreover, for the effective prevention and inspection on information security, several technical control measures have been implemented, for example, setting up door access control and monitors in the key areas and prohibiting copying and photographing.

## IT Security

*IT support is vital for the effective running of business activities within the company as the IT system carries a large amount of confidential information. A range of activities related to R&D, supply chain, and delivery of the company processes and procedures are supported and protected by the IT system. In this way, logs and records can be checked and traced with non-repudiation.*

*The ZTE desktop cloud and R&D cloud are built and standardized for use in key security protection fields such as in the R&D labs. All R&D activity is developed in the cloud, ensuring that product-related code and key documents are stored securely in the cloud platform. It is prohibited to copy and send information outside of the company without authorization. In addition, access to the Internet is not available to the desktop cloud and R&D cloud in secure areas. At the same time, the authority of the Internet access to the desktop cloud is disabled by default. Cloud desktops of different users are segregated in terms of memory and data. The code management server is only accessible through the desktop cloud environment for R&D personnel.*

*The Information Management Dept. of the company audits the networks with respect to major office systems, servers, and databases in a regular manner, and submits suggestions to responsible units and persons, urging them to rectify any concerns or issues within a specified period.*



## Asset Management

Asset management is the foundation of information security and any vulnerability, intrusion, or breach shall be located and handled based on the assets. From the perspective of information security, information assets refer to all things that are valuable to the company, including the physical area, personnel, electronic or paper documents, databases, software, hardware, mobile devices, applications and other information or information carriers. We have therefore classified the assets to help monitor and confirm accurate configuration information of ZTE assets. The responsibilities shall be defined for personnel so that an entire life cycle of asset management can be conducted.

All the hardware like the company's server and computers have a fixed asset number and label. The fixed asset administrator of a department is in charge of managing and checking the fixed assets. If hardware assets such as computers are brought out of the office area, they need to be logged on the system and submitted to relevant leaders in advance for authority to be granted. The security personnel should scan, identify, and confirm the asset labels.



## ID Authentication and Permission

---

The principle of identity authentication and minimum authorization management has been applied to IT protection on information security. For instance, after enrollment, each employee only has the basic and necessary permissions to the systems of finance, personnel, and IT while other special permissions need to be applied for on the IT website. The corresponding reasons ( job requirements) and authorization period need to be described in the application. After it is approved by a relevant responsible leader, a dedicated IT support person processes and configures the permission according to the person's role. The Information Management Dept. audit the permissions of the employees IT systems periodically.

There are security protection measures implemented in several ways to authenticate a user's identity. First, when logging into the company system through the account password, dual-factor authentication is performed. Second, a strong password policy is applied in setting the account password. Third, if the password is incorrectly entered over a set number of attempts, the account will be locked. Fourth, if the device is lost, approval will be required in the IT system prior to binding the data to another device.

Furthermore, some system permissions are valid in a certain periods and will be revoked automatically upon expiration. When the account permissions applied by employees comes into expiration or failure, like access permission to the Virtual Private Network (VPN) and mail outbound permission, they are revoked by the system automatically. The user needs to re-apply if they need to restore their permissions. When an employee resigns or transfers a position, the original corresponding permissions will be canceled. ZTE manage security risks to a largest degree by consistent control of our IT system.



## Network Security

---

ZTE has implemented relevant security measures to control the infrastructure network in terms of network access security, remote operation and maintenance security, and configuration security. The company provides a secure network environment for R&D, production, and operation services through measures such as access control, security segregation, and boundary protection.

Devices connected to the company network must meet the security baseline requirements and pass a user identity authentication. Before authorizing a connection, the system will automatically perform multiple security checks on the terminals. Only qualified terminals gain access to the ZTE network, where the desktop security software and document security software of the company are installed, security patches are automatically installed, anti-virus software is regularly upgraded, and high-risk software and software with intellectual property risk are not installed.

We have implemented network segregation to manage internal security threats on the network. For example, the R&D network and office network are isolated networks, and the production network and office network are isolated.

At the network boundary, firewall, intrusion detection and protection, and other automated detection tools are utilized. Under the strict monitoring of these tools, security threats outside the network are greatly reduced, and a secure network environment is created for R&D, production, and office work of the company.



## Personal Data Protection

*Against the backdrop of rapid development of communication network, big data, and cloud computing, more and more personal data is being collected, stored, transmitted, and used throughout networks. In order to protect the security of this important personal data, major countries and regions have promulgated a series of laws and regulations in the field of data protection, such as the General Data Protection Regulation (GDPR) by the European Union (EU), the California Consumer Privacy Act of 2018 by the United States, and China's Cybersecurity Law. For ZTE, data protection is not only a legal requirement, but also an important guarantee for corporate compliance governance and security management.*

*By incorporating data protection into the company's compliance system, ZTE has promoted the protection of personal information and guaranteed data security through focusing on the core scenarios, improving the organizations, introducing technical measures, and optimizing management methods. In addition, ZTE regards data protection as a self-commitment to cybersecurity. Therefore, the company has incorporated the concept of data protection into the product design and service delivery process, continuously satisfying the current requirement by global data protection regulations and going above and beyond these guiding regulations. ZTE plans to achieve a sustainable development strategy together with our global customers, suppliers and other partners that is secure and trusted.*

## Data Protection Compliance System

While establishing a complete compliance system in data protection, ZTE has implemented risk sorting, organized investigation and review in the fields of management, technology, service, procedure, product, and personnel, constructed and upgraded the agreement, standard, mechanism, tools, and teams, and formulated specific initiatives on the basis of risk level and holistic company compliance. To guide our data protection action, ZTE takes the EU GDPR as a benchmark standard for overall compliance, and takes into account the territorial control requirements of each country, so that the principles we adopt can be applicable to our global operations around the world.

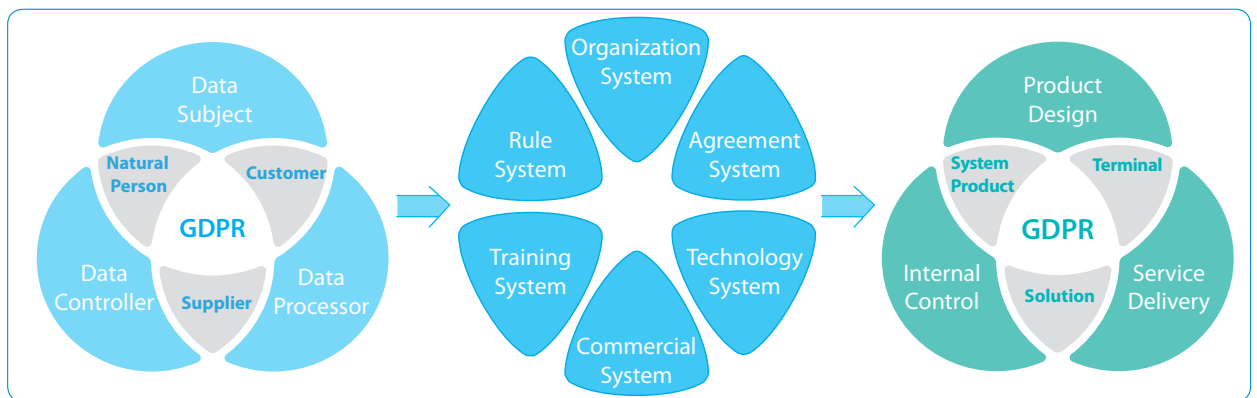


Figure 9 Data Protection System

ZTE has executed a series of specific improvements in data protection in the aspects of organization, rules, agreements, training, and technology. In terms of organization system, a mode of "support by a professional team, three lines of defense for control, and collaboration among multiple internal and external entities" has been established. ZTE has also constructed a four-level rule structure, "Policy, overall regulation, service guidelines, agreements and records", to help departments identify and respond to data protection risks in business activities based on their respective management scenarios. The agreement system acts as a key foundation of data compliance, allowing us to organize and promoted the signature of legally binding agreements in a unified manner.

As for the training system, an integrated mechanism of course development, training implementation, and effect supervision is established to raise an employee's awareness and capability in data protection compliance from multiple dimensions. In the technology system, we have actively adopted and continued to seek the best and applicable technical approach for data protection. Moreover, the compliance requirements are carried out with information system upgrading and professional tools. In a commercial system, we rely on a special compliance consulting service to execute the risk defense and control in the commercial processes such as major exhibitions and large-scale events.

Therefore, through systemic efforts, ZTE has established data protection compliance guidelines and standards that regulate our core business that helps functional units and all employees in their positions to understand our data protection principles, and to strictly follow the applicable regulations and procedures of the company. ZTE has also signed the Data Processing Agreement (DPA), Standard Contractual Clause (SCC, cross-border data transfer), supplemented by Notification Letter and Authorization Letter that are consistent with GDPR requirements. In addition, we have applied encryption, anonymity, and pseudonym security technologies, and taken such security measures as dual-factor authentication, permission management, and access monitoring, which will support the data protection and security defense in the processes of collection, storage, use, transfer, and destruction.

## Data Breach Protection Response Mechanism

The response to data breach has received the most attention in the entire compliance system in data protection. As a result of this, ZTE has built a mechanism for data breach incident response with quick collaboration between multiple parties at the core. Relatedly, we have specified the response procedures and developed a response system. The specific operation is supported by the data protection manager team extensively covering all business lines and regions as well as the specialist team and Data Protection Officer Team. In the event of a suspected incident, they will quickly process and organize responses, protect personal data in accordance with rules, reduce potential losses, and conduct the notification process. Meanwhile, the entire incident response process will be recorded in the specialized reporting system, to prepare the possible document referral and evidence submission to the regulatory agency. ZTE organizes incident response drills from time to time on data breaches and strengthens the effectiveness of daily post responsibility and incident response mechanism to prevent data breaches and handle data breaches in an organized manner.

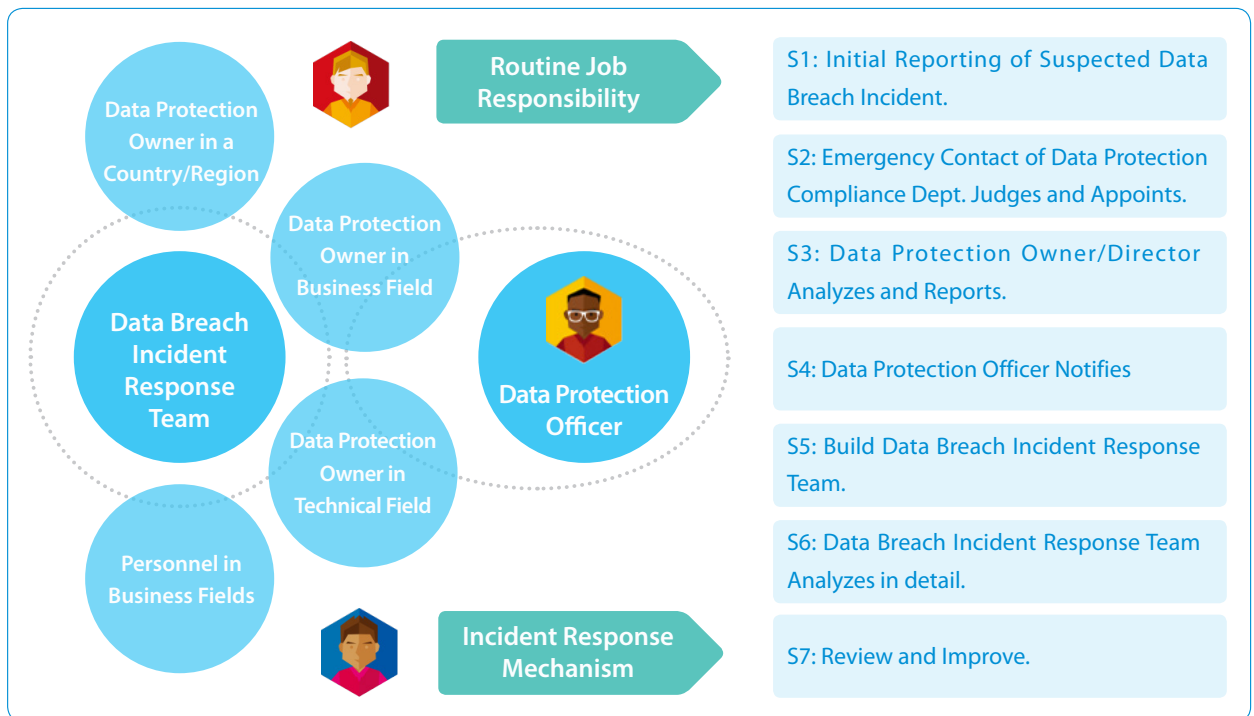


Figure 10 Data Breach Protection Response Mechanism

To ensure the implementation of each policy and initiative, ZTE has constructed a data protection audit mechanism and opened up channels for violation reporting. Specifically, ZTE has developed a full-time compliance audit team and incorporated the self-check and audit into the internal control and guarantee mechanism to carry out routine supervision and promote a positive cycle involving awareness building, resource investing, procedure re-creating, and capability upgrading for data protection.

## Data Protection Solution Practice

Based on innovative technical solutions, ZTE has practiced and incorporated the personal data protection requirements with cybersecurity requirements, and explored a secure and compliant product system and solutions system.

We have used personal data protection methods and practices during the product life cycle to raise the data protection compliance level. In compliance with principles of privacy by default and privacy by design, ZTE maintains the import of security control in the product design phase by adhering to the General Data Protection Impact Assessment Specification and Product Project Data Protection Impact Assessment. It takes personal data protection and security technology processing as the default attributes of cybersecurity to ensure that the personal data processing is performed in a legal, fair, and transparent way.

Based on a design of product data masking protection authorized by the customer, the data controller and data processor can interact with each other to ensure the security of multi-party services through the use of the authorization center, security network, network element masking, and security technology designs. In the case of remote access to the technical problem solution and incident response maintenance of the customers in the EU region, a remote access solution in the security mode is adopted based on the Cross-Border Data Transfer Agreement, so as to cooperate with the customer, EU local engineers and engineers at our Chinese headquarters, and carry out self-driven data protection practice.



# Security Incident Management

Cybersecurity can be influenced by many factors, for instance, threats, weaknesses, and cost benefit, so it is hard for us to eliminate all the security risks. When a security risk becomes a security incident, in addition to providing timely and effective responses, ZTE shall also cooperate with stakeholders to develop a solution in a short time period to reduce any negative impact caused by the security incident. Insisting on the principles of being open and transparent, ZTE ensures that it exposes all potential product vulnerabilities, including final solutions, to customers in a timely manner.

## Responses to Cybersecurity Incidents

ZTE's PSIRT team is responsible for receiving, processing and disclosing security vulnerabilities related to ZTE's products and solutions. Coordinating with customers and stakeholders, the PSIRT team quickly develops solutions. Creating a key security incident response mechanism for security incidents (for example, data breach) ensures a unified coordination, fast repair, and swift service recovery into effect.

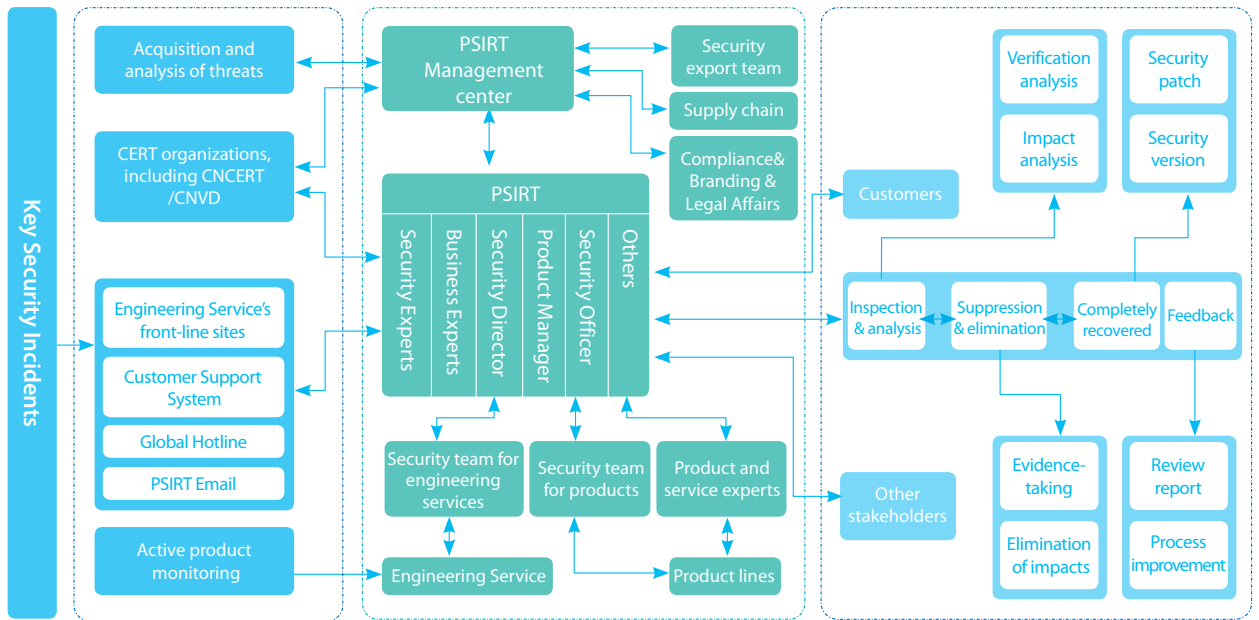


Figure 11 Key Security Incident Response Mechanism

For security incidents, a closed-loop management mechanism including measures for precautions, inspection, rectification, recovery, and response after the problem is solved has already been created. Once a security incident is reported based on the result of day-to-day product monitoring, the PSIRT team consisting of security experts, business experts, product security directors, the contact person of the PSIRT, and chief security officer, shall be formed in a very short time to analyze incident and take the necessary measures to control its development, and ensure that services are recovered. A review of the incident to improve the handling process and prevent similar incidents from occurring again after the incident to ensure effective control is implemented.



## Handling Process for Cybersecurity Vulnerabilities



ZTE actively strengthens its cooperation with external security organizations. For all the vulnerabilities that are identified from both inside and outside of ZTE, based on the principle of openness and transparency, ZTE ensures that they are disclosed with the relevant parties. As a member of the FIRST and a CVE Numbering Authority (CNA), ZTE is dedicated to publishing vulnerability exposure jointly with customers and stakeholders in a more open manner. Product vulnerabilities are disclosed on the websites of ZTE and CVE. To encourage both internal and external identification of product vulnerabilities, ZTE has formulated a vulnerability detection bounty program.

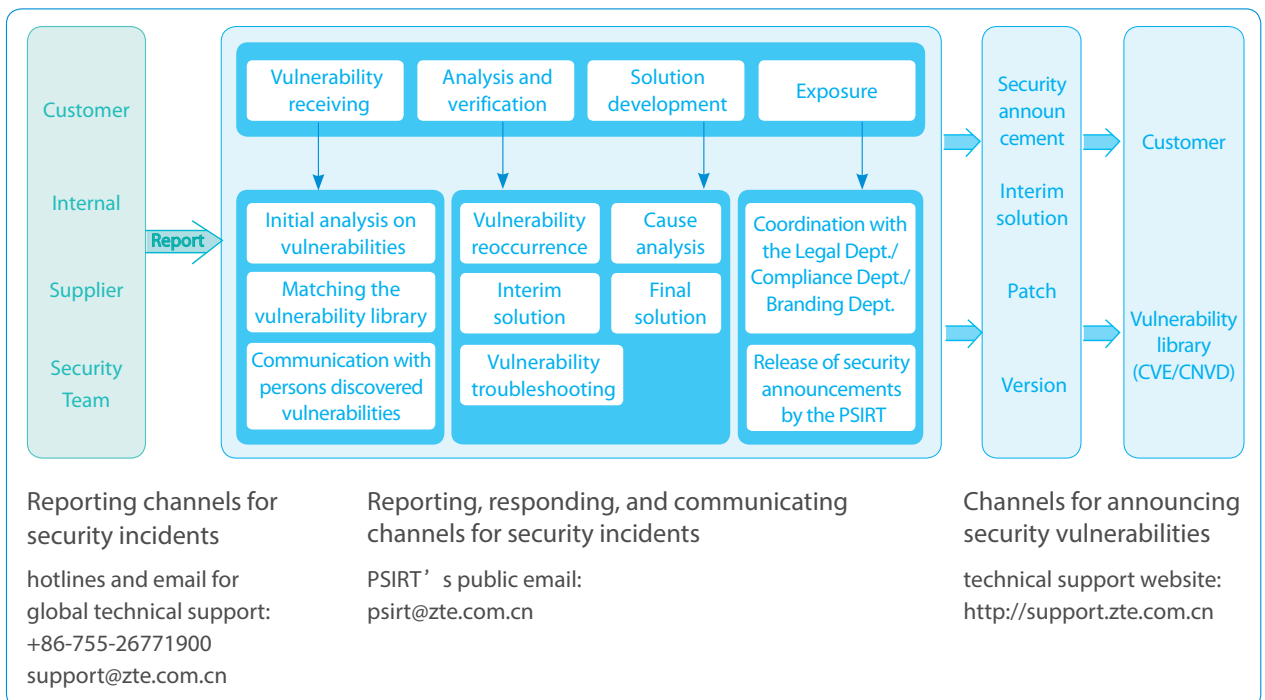


Figure 12 Handling Process for Cybersecurity Vulnerabilities

The PSIRT's vulnerability handling process includes the following five stages:



## Receiving Vulnerability Reports

---

Receive reports on security incidents or security vulnerabilities from both inside and outside of the company, including the reports from customers, external CERT, White Hats, security research groups, and internal employees. To encourage responsible disclosure, supplier shall be provided with reasonable time period to deal with and resolve problems prior to disclosure.



## Analysis and Verification

---

The PSIRT team starts investigation and analysis as soon as it receives a vulnerability report. It confirms the vulnerability and then rapidly defines its severity level. During the analysis and verification stage, the PSIRT team maintains communications with the reporter of the vulnerability to ensure the accuracy and timeliness of the vulnerability analysis process.



## Solution Development

---

The PSIRT process and R&D process are closely related. Once a vulnerability is confirmed, the relevant product teams must immediately activate the response mechanism to determine the cause, inspect unidentified related products, develop recovery solutions, and test the effectiveness of the solutions. For vulnerabilities already disclosed, the development of a solution including a temporary solution to address such vulnerabilities shall be prioritized to ensure rapid resolution.



## Disclosure

---

In the process of handling an incident, the PSIRT team shall actively communicate with the vulnerability reporters, the product development teams, and customers, to disclose the problems in a transparent and detailed manner, while providing them with policies and solutions to address the vulnerability.



## Feedback

---

Once a solution is implemented, its effectiveness must be monitored to ensure no additional issues are found, with iterative solutions applied should they be required. A "closed-loop management", of the incident review helps ZTE improve its product R&D continuously, and ensure customers' security is maintained across the entire product lifecycle, enhancing both quality and security.



## Business Continuity Management

*Business Continuity Management (BCM) is a process that examines various risk factors and the potential fragility of the business when faced with unpredicted situations. ZTE has established a business continuity mechanism and a set of solutions based on ISO 22301 to ensure that the company has the ability to maintain the delivery of products and services.*

*ZTE's BCM covers both the primary business processes (which includes R&D, supply chain, and engineering services) and the supporting business processes (which includes the IT system, finance, personnel, and compliance) across the product lifecycle.*

*The guidelines in ZTE's BCM process are: to take precautions, reduce risks, respond quickly, and continuously improve the BCM capability, so as to protect the interests of our employees, customers, shareholders, suppliers, and other stakeholders to the maximum extent possible.*

*BCM and the management of security incidents are important safeguards for secure products and services. The incident response process focuses ZTE's ability to respond quickly and effectively, mitigates the impacts of security incidents, ensures the rapid recovery of business, and provides the best opportunity to test the implementation of the business continuity plan. BCM safeguards the management of security incidents by activating the incident response mechanism and implementing the business continuity plan when security incidents that affect business occur.*

### BCM in R&D

ZTE's multiple R&D centers can act as a backup for one another in emergency circumstances to ensure the rapid recovery of business and continuity.

A series of incident management plans have been drafted to cope with contingencies. For third-party patent claims, regular inspections are carried out on the patents by R&D to avoid infringements and cross-licensing. To address the turnover risk of core personnel, a retention mechanism that focuses on key personnel has been developed. For major risks, KPIs are set for regular monitoring to avoid business disruption.



## BCM in Supply Chain

The BCM of ZTE's supply chain is implemented through the Warroom operation mechanism, during which measures are regularly taken against the identified material supply risks and crisis management measures are implemented to deal with emergencies.

ZTE has drawn up a risk map of supply resources for risk management and control. When different types of emergencies occur, the suppliers, materials and their codes, and products involved and the severity of the impact can be quickly identified with the help of the risk map, allowing an overall risk assessment to be done in a timely manner. In addition, the risk map provides the necessary data to strongly support the daily monitoring and prevention of material risks.

ZTE's manufacturing bases in Shenzhen, Heyuan, Changsha, and Nanjing can provide backup for one another in terms of factories, power, raw materials, and finished product warehouses. The manufacturing bases in Shenzhen, Nanjing, and Heyuan can provide backup for one another and even for the base in Changsha in terms of the PCBA business.

## BCM in Engineering Services

A series of business continuity tactics have been established for engineering services, namely, pre-event prevention and control, in-event response, and post-event reconstruction, all three areas that are systematically interconnected. Contingency plans are developed for multiple business scenarios based on the identified disasters and disaster drills are organized regularly to ensure the continuous effectiveness and validation of these of the plans.

Offsite backup for disaster recovery is achieved via our global service hotline to protect the customer services from being affected by business disruption. When a local overseas service hotlines break down, a global service hotline in China can provide alternative support services. In some overseas regional customer support centers, the Inbound Contact global service is applied to provide offsite backup for the hotlines to ensure that the coming calls can be answered by routing the calls to China in emergency circumstances.

## BCM in IT Systems

ZTE has established a three-local active-active data center: metropolitan active-active + offsite disaster recovery. For core business systems, the active-active architecture is applied at the enterprise data centers (EDCs) at ZTE bases located at Shenzhen Hi-Tech Industrial Park and Xili of Shenzhen. At the same time, a backup for disaster recovery is applied at the EDC in Nanjing to synchronize the production environment data to other EDCs, to cope with additional incident scenarios. The systematic integration of the metropolitan active-active and offsite disaster recovery centers effectively enhances the continuity of the core system.

The IT Dept. keeps updating the risk assessments and business impact analysis (BIA) plan, while organizing drills in different ways to deliver successful core system recovery scenarios every year. By summarizing and analyzing the results of the drills, the IT Dept. identifies any gaps with the actual demand and makes continuous improvements. The effective management of the continuity of IT systems provides strong support and significant protection for the steady and continuous operations of the company's business.

# Independent Security Assessment


Among the three risk management defense lines, independent security assessment is the second one that evaluates and supervises the front-line security practices. Independent security assessment reviews cybersecurity from multiple perspectives based on the principles of risk control. This second line of defense reduces security risks and implements the closed-loop management and tracking of the identified problems via a supervision and control mechanism, to realize continuous improvement of cybersecurity governance.


## Control Mechanism for Independent Security Assessment


During the process of cybersecurity governance, the second line of defense is set to avoid the failure of the security management and control mechanism of the first line of defense, and to identify and solve the risks in the business. The assessment and supervision of security and the right of veto of the second line of defense are applied to reduce the risks that fail to be identified or insufficiently implemented in the security practices of the first line of defense.


ZTE has developed an operational control mechanism for independent security assessment to ensure effective verification. The operational control mechanism is based on an independent, automated, comprehensive, and closed-loop system.

Independent: The security assessments of the second line of defense are completely separate from the business at the first line of defense and shall be reported to the Cyber Security Committee (CSC). The second line of defense has discretion over the process and the results of the assessments, which are not subject to the business in the first line of defense.

 **Independent**  
The security assessments of the second line of defense are completely separate from the business at the first line of defense and shall be reported to the Cyber Security Committee (CSC). The second line of defense has discretion over the process and the results of the assessments, which are not subject to the business in the first line of defense.

 **Automated**  
The second line of defense can directly take actions against any problems found in the assessments. For example, if there are issues that violate the company's red lines, the second line of defense will exercise its veto rights on behalf of ZTE to immediately suspend the offending business activities of the units involved, including stopping the release of software and other business, while requiring the units involved to develop a resolution within a specified period.

 **Comprehensive**  
The assessments of the second line of defense monitors the whole security process, management and control mechanism, and the final deliverables of the first defense line, focusing on the processes and results of the governance and characterized by all-around supervision.

 **Closed-loop**  
The assessments of the second line of defense implement closed-loop management and tracking of the problems identified, while paying attention to the resolution and the results of eliminating the defects. Only problems that have passed the verification can be defined as being settled.

## Process of Independent Security Assessment

ZTE's independent security verification follows a normative process that covers areas such as the supply chain, R&D, delivery, and incident response.

At the planning phase, random spot checks are carried out on the first-line products and service projects. Specific plans are developed based on the requirements for cybersecurity governance.

At the implementation phase, assessments are carried out from two perspectives.

<b>Process assessment</b>	Assesses the effectiveness of the implementation of the regulations and control points set by the business units.
<b>Product assessment</b>	Assesses the security of the products and systems and conducting analysis and evaluation such as vulnerability scanning, security code audits, and the robustness testing of the protocols.

During the result review and reporting phase, reviews are done on the assessment results and the final results are reported to the CSC. In addition, the product vulnerabilities found will be reported in the defect management system. Closed-loop tracking will be carried out on the analysis, to ensure improvement, and verification of the vulnerabilities.

At the verification phase, inspections are performed on the improvements made and another spot check will be carried out on site when necessary. Verification shall be carried out on the correction of the product defects, which will be tracked through the defect management system until the defects are resolved.

## Methods Applied in Independent Security Assessment

Multiple methods are applied in the independent security assessment for evaluation and verification, for example, tests for the functions of security baselines, security scanning, and penetration tests. In this way, the effectiveness of the security governance of the first-line products is verified from multiple perspectives.

### Tests for the Functions of Security Baselines

Carried out according to the security requirement baselines to verify the actual status of the security functions specified in the baselines and the effectiveness of such security functions.

### Security Scanning

Industrial-wide accepted scanning tools are adopted to verify the results of the first line security practices, including scanning and auditing the security of the product source code, and scanning the operating systems, databases, WEB services, and other third-party modules, to identify the vulnerabilities of the systems and devices.

### Penetration Tests

Simulated attack tests are carried out on products and systems, which will, through the analysis of the real operational scenarios of the products and systems, analyze the potential weaknesses, detect security vulnerabilities, carry out defect analysis, and put forth improvement suggestions.

# Security Audit

Cybersecurity audit provides reasonable assurance for the company's management, customers, and other interested parties that the policies, regulations, and process of cybersecurity have been implemented effectively to satisfy customer needs. As a third line of defense for cybersecurity governance, security audits to carry out independent evaluation on the robustness, rationality, and effectiveness of the company's cybersecurity system, to prompt the company to strengthen the construction of the cybersecurity system to implement the system stringently, ensure the continuous and effective improvements made to the system, and to realize supervision and transparent management of the system.

ZTE has always held an open and transparent attitude towards its key stakeholders, receiving internal audits and external audits according to the company's articles of association. Audit reports are submitted to the Chairman for approval. Regular reports are submitted to the Audit Committee or the Board of Directors. Risks found in the audits are reported to the management and Board of Directors in a timely manner.

ZTE's security audits are carried out from multiple perspectives, including organization and operation, risk management processes, control activities, and internal supervision, covering the end-to-end cybersecurity processes which include R&D security, supply chain security, delivery security, security incident response, and independent security verification.



## Audits of Organization and Operation

Focus on integrated operational management, competences, reporting and decision-making mechanism for important issues of cybersecurity, etc.



## Audits of Risk Management

Focus on identification, evaluation, the handling of cybersecurity risks, the establishment and implementation of the risk warning mechanism, contingency plans and procedures, and the backtracking mechanism for security loss incidents.



## Audits of the Effectiveness

Control activities focus on the design of control points and their application in the business process, and the effective implementation of the control points.



## Audits of Internal Supervision

Focus on daily supervision and special supervision mechanism for the first and second lines of defense, correction of the problems found, and construction and implementation of the evaluation mechanism.

The whole audit process is geared towards risks. ZTE continuously reviews the robustness and effectiveness of the company's cybersecurity system to satisfy the security requirements of the customers and other stakeholders.

## Cybersecurity Labs and External Cooperation

*ZTE continuously benchmarks itself against security standards and best practices, cooperates with organizations of the industry actively, and puts efforts into communicating with customers and other stakeholders in an open and transparent manner and boosting mutual trust, to realize the common goal of resisting cybersecurity threats.*

*Cybersecurity lab is one of the measures taken by ZTE to increase transparency around the globe. The cybersecurity lab will operate in a "1+N" mode, with the core lab established in China and multiple remote access points set in China and other countries. With the geographical advantages brought about by a multi-country deployment, the cybersecurity lab will provides external security assessment services for global customers, regulators, and other stakeholders by opening up product source code and documents, and by providing multi-dimensional security assessment services.*

*These cybersecurity labs will be a physical platform to enable ZTE's external audits and independent verification, creating an open, transparent, and secure environment for the first and second lines of defense to carry out their functions. The three pre-set functions of the cybersecurity lab are:*

- Reviewing and evaluating the source code of ZTE's products in a secure environment.*
- Providing access to important technical documents of ZTE's products and services.*
- Enabling security tests on ZTE's products and services carried out manually or with the help of automated tools.*

*At the same time, ZTE are seeking to build strategic partnership with third parties. The technologies and services acquired from such partnership will be applied in the development of the cybersecurity labs, enabling independent security verification, validation, and independent security audits.*





# Look Forward and Advance Together

*After years of practical implementation, technological innovation, and accumulation of a wealth of experience, ZTE has developed the competencies to provide end-to-end security solutions that covers core 5G technologies, cybersecurity operations, and industry applications. 5G is characterized by extensive connection capabilities, low delay, high speed, data throughput, a wide scope of industry coverage, and the internet of everything, and is deeply integrated with technologies such as cloud computing, big data, artificial intelligence, and virtual reality. In the coming decade, the mobile network will serve various industries, things will be connected more closely and extensively, the network will cover a wider scope, and there will be more applications, which means that we will be confronted with more security challenges.*

*ZTE will keep investing resources in the research of security technologies and methods, maintain constant self-innovation, introduce and learn from advanced ideas and methods of cybersecurity governance, comprehensively enhance cybersecurity and our service capability, to satisfy the security needs of the new technologies, applications, and models. We have to embrace the idea of transparency, openness, trust, and cooperation, carry out closer cooperation with our customers, partners, governments, suppliers, and standardization organizations, to facilitate end-to-end security practices, cope with the challenges in a calm manner, and provide secure and trustworthy products and services to industry.*





**Table1 Acronyms and Symbols**

Acronym or Symbol	Full Name
3GPP	3 <sup>rd</sup> Generation Partnership Project
5G	5 <sup>th</sup> generation mobile communication
AEO	Authorized Economic Operator
BCM	Business Continuity Management
CC	Common Criteria
CERT	Computer Emergency Response Team
CNA	CVE Numbering Authorities
COP	Communities of Practice
CSA	Cloud Security Alliance
CSC	Cyber Security Committee
CVE	Common Vulnerabilities & Exposures
CWE	Common Weakness Enumeration
EDC	Enterprise Data Center
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
HPPD	High Performance Product Development
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
PSIRT	Product Security Incident Response Team
SATRC	S: System A: Asset T: Threat R: Risk C: Control
SSG	Software Security Group
STIG	Security Technical Implementation Guide

# Appendix: Major Cybersecurity Events of ZTE

2005

ZTE passed the ISO 27001 certification (Information Security Management System), which covered all the business of ZTE. In 2014, ZTE has upgraded to pass the ISO 27001: 2013 certification. In 2017, ZTE has been certified with ISO 27001: 2013 in multiple countries, including China, India, the U.S., Germany, Netherlands, the U.K., France, and Italy. As of March, 2019, 14 newly established subsidiaries in Europe passed the ISO 27001: 2013 certification in such countries as Austria, Greece, Spain, and Belgium.

ZTE took on the position of the Vice Chairman of ITU-T SG17. ZTE had long been active in international standards organizations such as 3GPP, IETF, ITU-T, and CSA, and security forums, playing a role in promoting the standardization work in the security field.

2011

ZTE established the CSC that carried out cybersecurity program.

ZTE started to certify network management products with the Common Criteria (CC). As of the end of 2018, 12 types of products were certified by the CC, including such mainstream products and devices as the core network, access network, optical transmission, network management, router, and base station controller.

2013

ZTE established the cybersecurity lab, which was an independent security verification body within the company that provided an integrated platform for security assessments, development of security capability, security incident response, management of security knowledge, and technology exchanges.

2014

ZTE released a series of internal standards and regulations, including the General Requirements and Framework for Product Security and Security Baselines.

2015

ZTE joined the Forum of Incident Response and Security Teams (FIRST), with an aim to enhance its response capability of security incidents.

2017

ZTE passed the ISO 28000 (Supply Chain Security Management System) certification, which covered the procurement, manufacturing, and logistics of 26 types of telecommunication products (including mobile devices). In 2017, ZTE was granted with the Certificate of Authorized Economic Operator (AEO) issued by the World Customs Organization.

ZTE established a comprehensive cybersecurity system that covered multiple areas, including R&D, supply chain, engineering services, security incident response, and independent security verification.

ZTE became one of the CVE Numbering Authorities (CNA). The CNA provided channels for proactive disclosure of security vulnerabilities.

2018

ZTE released its product security red lines.

ZTE made adjustments to the CSC, the members of which are the top management. The organization and deployment of security assurance has run through the management levels.

ZTE designated Zhong Hong as the Chief Security Officer of the company.

ZTE started to establish a cybersecurity lab that will be operated in the "1+N" mode. The core lab was set in China, and multiple remote access points were set in China and other countries. In 2019, ZTE will establish two cybersecurity laboratories in Belgium and Italy, where source code auditing, security design review, and security testing will be carried out.

# Leading 5G Innovations

